

STIC Search Report

STIC Database Tracking Nur

TO: Michael Cuff Location: 5D29 Art Unit: 3627

Case Serial Number: 09/839471

From: Joan Goodbody Location: EIC 3600

Knox 4B71

Phone: 571-272-8592

joan.goodbody@uspto.gov

Search Notes

Dear Michael:

Attached are the results of your search request regarding

SYSTEM AND METHOD FOR DEBIT ACCOUNT TRANSACTIONS

Please let, me know if you need anything further.

Joan Goodbody







STIC EIC 3600 Search Request Form

Today's Date:	Class/Subclass	What date would you like to use to limit the search? Priority Date: $6/18/98$ Other:
Name Michae	1 Cuff	Format for Search Results (Circle One):
AU 3627	Examiner # <u>7449</u>	PAPER DISK EMAIL Where have you searched so far?
Boom # KNX 5-1	029 Phone 2-677	18 DWPL FPO JPO ACM IBM TDB

Room # <u>MNX5-D29</u> Phone <u>2-6778</u>

Serial # <u>09/839, 47/</u>

Serial # <u>DWPI EPO JPO ACM</u>

IEEE INSPEC SPI Other Full Business methods

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

Claims 6 is attached Major elements required

A host server

Means for establishing a debit account with a

means for establishing a debit account with a

unique account number,

means for the PIN to be customer selected and

means for the PIN to be customer selected and

assigned at the terminal and during the

transaction.

STIC Searcher _____ Phone _____ Date picked up _____ Date Completed____



Appl. No. 09/839,471 Amdt. dated Reply to Office action of September 25, 2006

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1. (Cancelled)
- 2. (Cancelled)
- 3. (Cancelled)
- 4. (Cancelled)
- 5. (Cancelled)
- 6. (Previously Amended) A system for establishing a debit account via a point of sale transaction comprising:
- (a) a transaction terminal, said terminal including inputmeans, display means, and processing means;
- (b) printing means operatively coupled to said transaction terminal;
- (c) communications means integral to said transaction terminal;
- (d) a secure host server in communication with said transaction terminal;
- (e) said transaction terminal including: means for initiating said point of sale transaction to accept funds from a customer to be deposited into a debit account; means for accepting an input value representing funds to be deposited into said debit account;

Appl. No. 09/839,471 Amdt. dated Reply to Office action of September 25, 2006

means for accessing said secure host server via said communications means; means for transmitting said input value to said secure host server; means for receiving a debit account number unique to said transaction; means to assign a customer selected personal identification number (PIN) to said debit account number during said transaction; and means for providing said debit account number and said PIN to said customer in readable format.

- 7. (Previously amended) The system of claim 6, wherein said secure host server is operatively coupled to a processing means; said processing means including: means for creating a debit account specific to said transaction, means for assigning a unique debit account number [[with]] to said debit account; and means for storing an electronic representation of currency equivalent to the input value into said debit account; and means for associating said personal identification number (PIN) with said debit account.
- 8. (Previously amended) The system of claim 6, further comprising a database for storing said debit account number, said database further including account balance information associated with said debit account number, wherein said funds can be withdrawn from said debit account by a customer using said debit account number and said PIN.







United States Patent and Trademark Office

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
WWW.usplo.gov

CONFIRMATION NO. 2469

SERIAL NUMBI 09/839,471	ER	FILING DATE 04/19/2001 RULE	(CLASS 705	GRO	UP AR 2167	T UNIT		ATTORNEY OCKET NO. 2240.004
** CONTINUING THIS APPL WHICH CL ** FOREIGN APF	DAT ICA AIMS	FION IS A CIP OF 09/ B BENEFIT OF 60/089 ATIONS **********	(334,887 9,755 06 *****						
GRANTED ** 06/ Foreign Priority claimed 35 USC 119 (a-d) condimet Verified and Acknowledged	13/20	yes no no Met after Allowance		** SMALL E STATE OR COUNTRY FL	SHE DRAN	Y ** ETS WING	TOTA CLAIN 21		INDEPENDENT CLAIMS 3
ADDRESS Michael A. Slavin McHale & Slavin, Suite 402 4440 PGA Blvd. Plam Beach Gard	P.A.	71 0	191	7				•	
TITLE System and meth	od fo	or debit account transa	actions						
FILING FEE RECEIVED No to charge/credit DEPOSIT ACCOUNT No for following:					UNT	1.1 time)	18 Fees ((Prod	cessing Ext. of



STIC Search Results Feedback Form

EIC 3600

Questions about the scope or the results of the search? Contact the EIC searcher or contact:

Karen Lehman, EIC 3600 Team Leader KNX 4A58, 571-271-3496

Voluntary Results Feedback Form
► I am an examiner in Workgroup: Example: 3620 (optional)
Relevant prior art found , search results used as follows:
☐ 102 rejection
103 rejection
Cited as being of interest.
Helped examiner better understand the invention.
Helped examiner better understand the state of the art in their technology.
Types of relevant prior art found:
☐ Foreign Patent(s)
 Non-Patent Literature (journal articles, conference proceedings, new product announcements etc.)
> Relevant prior art not found:
Results verified the lack of relevant prior art (helped determine patentability).
Results were not useful in determining patentability or understanding the invention.
Comments:

Drop off or send completed forms to ElC3600 PK5 Suite 804



Day: Wednesday

Date: 2/7/2007 Time: 10:38:02

PALM INTRANET

Application Number Information

Application Number: 09/839471

Assignments

Filing or 371(c) Date: 04/19/2001

Effective Date: 04/19/2001

Application Received: 04/23/2001

Pat. Num./Pub. Num: /20010023415

Issue Date: 00/00/0000

Date of Abandonment: 00/00/0000

Attorney Docket Number: 2240.004

Status: 71 /RESPONSE TO NON-FINAL OFFICE ACTION

ENTERED AND FORWARDED TO EXAMINER

Confirmation Number: 2469

Examiner Number: 74494 / CUFF, MICHAEL

Group Art Unit: 3627

Class/Subclass:

705/021.000

Lost Case: NO

Oral Hearing: NO

Interference Number:

Unmatched Petition: YES L&R Code: Secrecy Code:1

Third Level Review: NO

Status Date: 10/18/2006

Waiting for Response

Req for Continue

Secrecy Order: NO

IFW IMAGE

Desc.

Title of Invention: SYSTEM AND METHOD FOR DEBIT ACCOUNT TRANSACTIONS

Bar Code PALM Location Location Date Charge to Loc Charge to Name Employ	yee Name Location
Appln Contents Petition Info Atty/Agent Info Continuity/Reexam	. Foreign Data
Search Another: Application# Search or Patent#	Search
PCT / Search or PG PUBS #	Search
Attorney Docket # Search	
Bar Code # Search	

To go back use Back button on your browser toolbar.

Back to PALM | ASSIGNMENT | OASIS | Home page

Set Items Description
S1 75 S AU=(KEIL D? OR KEIL, D? OR KEIL(2N)DEAN)
S2 2 S S1 AND IC=G06F-017/60
; show files

[File 350] **Derwent WPIX** 1963-2006/UD=200709

(c) 2007 The Thomson Corporation. All rights reserved.

*File 350: DWPI has been enhanced to extend content and functionality of the database. For more info, visit http://www.dialog.com/dwpi/.

[File 347] JAPIO Dec 1976-2006/Oct(Updated 070201)

(c) 2007 JPO & JAPIO. All rights reserved.

2/5/1 (Item 1 from file: 350) **Links**

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012274733 *Drawing available* WPI Acc no: 2002-215396/200227

Related WPI Acc No: 2001-146877; 2002-215394

XRPX Acc No: N2002-164957

Debit account establishing system for credit card transaction, sends unique personal identifier number corresponding to debit account number in readable format from server to customer, based on received funds

Patent Assignee: KEIL D S (KEIL-I)

Inventor: KEIL D S

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20010023415	A1	20010920	US 199889755	P	19980618	200227	В
7			US 1999334887	A	19990617		
			US 2001839471	A	20010419		

Priority Applications (no., kind, date): US 1999334887 A 19990617; US 199889755 P 19980618; US 2001839471 A 20010419

Patent Details

Patent Number	Kind	Lan	Pgs Draw Filing Notes		Filing Notes			
US 20010023415	A 1	EN	15	8	Related to Provisional	US 199889755		
					C-I-P of application	US 1999334887		

Alerting Abstract US Al

NOVELTY - A transaction terminal initiates point of sale transaction to accept input funds to be deposited into debit account from a customer. The terminal transmits input value of funds to host server which in turn sends unique personal identifier number (PIN) corresponding to debit account number in a readable format to the customer. DESCRIPTION - An INDEPENDENT CLAIM is also included for debit account establishment method. USE - For establishing debit account for credit card ATM, bank card, prepaid cards transaction. ADVANTAGE - Allows customer to establish debit accounts in easy and efficient manner, without providing

ADVANTAGE - Allows customer to establish debit accounts in easy and efficient manner, without providing personal identification data, thereby assuring anonymity of account. Since the system does not require the standard POS payment implements such as plastic card, smart card, etc., outlay of capital customer is minimized, and possibility of theft of card is eliminated.

DESCRIPTION OF DRAWINGS - The figure shows the transaction and funds flow of debit account establishing system.

Title Terms /Index Terms/Additional Words: DEBIT; ACCOUNT; ESTABLISH; SYSTEM; CREDIT; CARD; TRANSACTION; SEND; UNIQUE; PERSON; IDENTIFY; NUMBER; CORRESPOND; READ; FORMAT; SERVE; CUSTOMER; BASED; RECEIVE; FUND

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-017/60			Main		"Version 7"

US Classification, Issued: 705044000

File Segment: EPI; DWPI Class: T01; T05

Manual Codes (EPI/S-X): T01-N01A1; T01-N01A2A; T05-H02C3; T05-L01D

2/5/2 (Item 2 from file: 350) **Links**

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012274731 *Drawing available* WPI Acc no: 2002-215394/200227

Related WPI Acc No: 2001-146877; 2002-215396

XRPX Acc No: N2002-164955

Debit account establishing apparatus for credit card transaction, sends receipt printed with personal identifier and debit account numbers to transaction terminal, depending on received funds from customer

Patent Assignee: KEIL D S (KEIL-I)

Inventor: KEIL D S

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20010023409	Αl	20010920	US 199889755	P	19980618	200227	В
			US 1999334887	Α	19990617		
			US 2001837926	A	20010418		

Priority Applications (no., kind, daté): US 1999334887 A 19990617; US 199889755 P 19980618; US 2001837926 A 20010418

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes		
US 20010023409	Αl	EN	15	8	Related to Provisional	US 199889755	
					C-I-P of application	US 1999334887	

Alerting Abstract US A1

NOVELTY - A transaction terminal initiates point of sale (POS) transaction to accept an input value representing funds to be deposited into debit account, from a customer. The terminal transmits input value to host which in turn sends receipt printed with personal identifier number (PIN) and debit account number, to the customer.

USE - For establishing debit account through point-of-sale (POS) terminal for credit card, bank card, ATM debit

pre-paid cards transactions, etc.

ADVANTAGE - Allows customers to establish debit accounts in easy and efficient manner, without providing personal identification data, thereby assuring anonymity of account. The system does not require standard POS payment implements such as plastic card, smart card, etc., outlay of capital of customer is minimized and possibility of theft of card is eliminated.

DESCRIPTION OF DRAWINGS - The figure shows a block diagram of POS transaction terminal.

Title Terms /Index Terms/Additional Words: DEBIT; ACCOUNT; ESTABLISH; APPARATUS; CREDIT; CARD; TRANSACTION; SEND; RECEIPT; PRINT; PERSON; IDENTIFY; NUMBER; TERMINAL; DEPEND; RECEIVE; FUND; CUSTOMER

Class Codes

International Patent Classification

IPC	Class Level Scope		Position Status		Version Date	
G06F-017/60			Main		"Version 7"	

US Classification, Issued: 705017000, 705039000, 705016000

File Segment: EPI; DWPI Class: T01; T05

Manual Codes (EPI/S-X): T01-J12C; T01-N01A2A; T05-H02C3; T05-H02C5C; T05-L01D

```
? ds
Set Items Description
S1     25     S AU=(KEIL D? OR KEIL, D? OR KEIL(2N)DEAN)
S2     0     S S1 AND IC=G06F-017/60
S3     1     S S1 AND IC=G06F
; show files.
```

[File 348] EUROPEAN PATENTS 1978-2007/ 200705

(c) 2007 European Patent Office. All rights reserved.

*File 348: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.

[File 349] PCT FULLTEXT 1979-2007/UB=20070201UT=20070125

(c) 2007 WIPO/Thomson. All rights reserved.

^{*}File 349: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.

3/3K/1 (Item 1 from file: 348) Links

EUROPEAN PATENTS

(c) 2007 European Patent Office. All rights reserved.

01391338

Multiprocessor emulation support using dynamic linking

Mehrprozessorenemulationunterstutzung mit dynamischen Verbindungen Assistance a l'emulation d'un multiprocesseur par liaison dynamique

Patent Assignee:

• Texas Instruments Incorporated; (279078)

7839 Churchill Way, Mail Station 3999; Dallas, Texas 75251; (US) (Applicant designated States: all)

Inventor:

• Deao, Douglas

4574 Sheraton Circle; Texas 77423, Brookshire; (US)

• Keil, Deborah

113 Marc Drive Pittsburgh; 15236, Pennsylvania; (US)

• McGowan, Robert

3930 Monroeville Blvd, Apt.H9; 15146, Monroeville; (US)

McLean, Craig

5 Penn Towne Drive; 15642, Irwin; (US)

• Swoboda, Gary

4435 Balboa Drive; 77479-2130, Sugarland; (US)

• Szwewrenko, Leland

1234 N. Highland Avenue; 15206, Pittsburgh; (US)

• ...US)

• Keil, Deborah...

;;

Legal Representative:

• Holt, Michael et al (50422)

Texas Instruments Ltd., EPD MS/13, 800 Pavilion Drive; Northampton Business Park, Northampton NN4 7YL; (GB)

	Country	Number	Kind	Date	
Patent	EP	1179775	A2	20020213	(Basic)
Application	EP	2001000354		20010808	
Priorities	US	223697		20000808	
	US	887504	Р	20010622	

Designated States:

AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR;

Extended Designated States:

AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-011/26; G06F-011/26Abstract Word Count: 131

NOTE: 1

NOTE: Figure number on first page: 1

Type	Pub. Date	Kind	Text
Publication: English			

Procedural: English Application: English

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200207	643
SPEC A	(English)	200207	2008
Total Word Count (Document A) 2651			·
Total Word Count (Document B) 0			!
Total Word Count (All Documents) 2651		·	

```
Description
Set
        Items
                S AU=(KEIL D? OR KEIL, D? OR KEIL(2N)DEAN)
S1
                S S1 AND (ACCOUNT? ?(10N)TRANSACTION? ?)
S2
                S S1 AND ACCOUNT? ?
S3
                S S1 AND DEBIT
S4
                S S1 NOT PY>1998
·S5
           46
                   (unique items)
           44
S6
 ; show files
```

[File 2] INSPEC 1898-2007/Jan W4

(c) 2007 Institution of Electrical Engineers. All rights reserved.

[File 35] Dissertation Abs Online 1861-2007/Jan

(c) 2007 ProQuest Info&Learning. All rights reserved.

[File 65] Inside Conferences 1993-2007/Feb 05

(c) 2007 BLDSC all rts. reserv. All rights reserved.

[File 99] Wilson Appl. Sci & Tech Abs 1983-2007/Jan

(c) 2007 The HW Wilson Co. All rights reserved.

[File 139] EconLit 1969-2007/Jan

(c) 2007 American Economic Association. All rights reserved.

[File 474] New York Times Abs 1969-2007/Feb 04

(c) 2007 The New York Times. All rights reserved.

[File 475] Wall Street Journal Abs 1973-2007/Feb 03

(c) 2007 The New York Times. All rights reserved.

[File 583] Gale Group Globalbase(TM) 1986-2002/Dec 13

(c) 2002 The Gale Group. All rights reserved.

^{*}File 583: This file is no longer updating as of 12-13-2002.

6/6, AU, PY/1 (Item 1 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved. 07460275 INSPEC Abstract Number: B2000-02-2550E-067

Title: Profile control of sub-0.3 mu m contact etch features in a medium-density oxide etch reactor Author Keil, D.; Cooperberg, D.; Li, L.; Mueller, G.; Nguyen, T.; Khajehnouri, K.; Vahedi, V.; Hills, G.

Editor(s): Mathad, G.S.; Misra, D.; Sundaram, K.B.

Publication Date: 1998

1998

Copyright 2000, IEE

6/6, AU, PY/2 (Item 2 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

07208525 INSPEC Abstract Number: A1999-09-6480-013

Title: Microstructural evaluation of sintered nanoscale SiC powders prepared by various processing routes Author Schmidt, W.R.; McCarthy, G.; Palosz, B.; Stel'makh, S.; Aloshina, M.; Gierlotka, S.; Zinn, P.; Keil, D.G.; Calcote, H.F.

Editor(s): Gonsalves, K.E.; Baraton, M.-I.; Singh, R.; Hofmann, H.; Chen, J.X.; Akkara, J.A.

Publication Date: 1998

1998

Copyright 1999, IEE

6/6.AU.PY/3 (Item 3 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

06994717 INSPEC Abstract Number: A9818-6250-005

Title: Evolution of disordering in SiC under high pressure high temperature conditions: in-situ powder diffraction study

Author Palosz, B.; Stel'makh, S.; Gierlotka, S.; Aloszyna, M.; Pielaszek, R.; Zinn, P.; Peun, T.; Bismayer, U.; Keil, D.G.

Publication Date: 1998

1998

Copyright 1998, FIZ Karlsruhe

6/6, AU, PY/4 (Item 4 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

06776734 INSPEC Abstract Number: A9802-2852-034

Title: Edge-plasma trapping induced by ICRH in an end cell of a tandem mirror

Author Keil, D.; Cui, B.; Hershkowitz, N.

Publication Date: Nov. 1997

1997

Copyright 1997, IEE

6/6, AU, PY/5 (Item 5 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved. 06628381 INSPEC Abstract Number: B9708-2860-012

Title: Plasma etch processing of advanced ferroelectric devices

Author Cofer, A.; Rajora, P.; DeOrnellas, S.; Keil, D.

Publication Date: 1997

1997

Copyright 1997, IEE

6/6, AU, PY/6 (Item 6 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

06590865 INSPEC Abstract Number: B9707-2860-012

Title: The etching of platinum electrodes for PZT based ferroelectric devices

Author Keil, D.; Cofer, A.; Rajora, P.; DeOrnellas, S.

Editor(s): Mathad, G.S.; Meyyappan, M.

Publication Date: 1996

1996

Copyright 1997, IEE

6/6, AU, PY/7 (Item 7 from file: 2) Links

· INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

06533298 INSPEC Abstract Number: A9709-8120L-016

Title: Flame synthesis of high purity, nanosized crystalline silicon carbide powder

Author Keil, D.G.; Calcote, H.F.; Gill, R.J.

Editor(s): Hepp, A.F.; Kumta, P.N.; Sullivan, J.J.; Fischman, G.S.; Kaloyeros, A.E.

Publication Date: 1996

1996

Copyright 1997, IEE

6/6, AU, PY/8 (Item 8 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

06533297 INSPEC Abstract Number: A9709-8120L-015

Title: Combustion synthesis of nanosized SiC/sub x/N/sub y/ powder's

Author Keil, D.G.; Calcote, H.F.; Gill, R.J.

Editor(s): Hepp, A.F.; Kumta, P.N.; Sullivan, J.J.; Fischman, G.S.; Kaloyeros, A.E.

Publication Date: 1996

1996

Copyright 1997, IEE

6/6, AU, PY/9 (Item 9 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

05520851 INSPEC Abstract Number: A9324-5255-004

Title: A study of a parallel mode launch into a magnetic beach

Author Keil, D.; Bettenhausen, M.H.; Hershkowitz, N.

Publication Date: June 1993

1993

6/6, AU, PY/10 (Item 10 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

05278661 INSPEC Abstract Number: A9224-5235-021

Title: Observation of whistler instability in the Phaedrus-B tandem mirror plasma

Author Cui, B.; Hershkowitz, N.; Roberts, D.R.; Litwin, C.; Keil, D.

Publication Date: Sept. 1992

1992

6/6, AU, PY/11 (Item 11 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

05163243 INSPEC Abstract Number: A9213-5255-013

Title: Radial diffusion induced by an ion cyclotron resonance layer in the Phaedrus-B tandem mirror

Author Ichimura, M.; Yun-Jian Wen; Brouchous, D.A.; Breun, R.A.; Hershkowitz, N.; Probert, P.; Majeski, R.;

Intrator, T.; Roberts, D.; Keil, D. Publication Date: April 1992

1992

6/6, AU, PY/12 (Item 12 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

04614490 INSPEC Abstract Number: A90061227

Title: Radial ion diffusion induced by cyclotron resonance heating at the thermal barrier region in the

Phaedrus-B tandem mirror

Author Wen, Y.-J.; Brouchous, D.; Ichimura, M.; Breun, R.A.; Hershkowitz, N.; Probert, P.; Majeski, R.; Intrator,

T.; Roberts, D.; Keil, D. Publication Date: 1989

1989

6/6, AU, PY/13 (Item 13 from file: 2) **Links**

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

04613068 INSPEC Abstract Number: A90061210

Title: Improved MHD stabilization in the Phaedrus-B tandem mirror obtained by using ICRF excited by rotating field antennas and measurements of a model antenna near fields

Author Hershkowitz, N.; Breun, R.A.; Brooker, P.; Browning, J.; Brouchous, D.; Conrad, J.R.; Cui, B.S.; Ferron, J.; Goulding, R.H.; Intrator, T.; Keil, D.; Litwin, C.; Majeski, R.; Meassick, S.; Nelson, B.; Persing, H.; Probert, P.;

Roberts, D.; Tataronis, J.A.; Yunjian Wen; Yasaka, Y.

Publication Date: 1988

1988

6/6, AU, PY/14 (Item 14 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

04600698 INSPEC Abstract Number: A90053724

Title: Radial transport in the Phaedrus-B tandem mirror

Author Breun, R.A.; Hershkowitz, N.; Brooker, P.; Browning, J.; Brouchous, D.; Conrad, J.R.; Cui, B.J.; Edgell, D.; Ferron, J.; Goulding, R.H.; Intrator, T.; Keil, D.; Majeski, R.; Meassick, S.; Peng, L.L.; Persing, H.; Probert, P.; Roberts, D.; Wen, Y.

Publication Date: 1988

1988

6/6.AU.PY/15 (Item 15 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

04376298 INSPEC Abstract Number: A89065584

Title: Whistler-mode electron cyclotron emission from the Phaedrus-B end cell

Author Cui, B.; Probert, P.H.; Brooker, P.D.; Nonn, P.D.; Keil, D.L.; Hershkowitz, N.; Majeski, R.P.; Breun, R.A.; Ellis, R.F.

Publication Date: Feb. 1989

1989

6/6, AU, PY/16 (Item 16 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

04166819 INSPEC Abstract Number: A88085512

Title: Experimental results from Phaedrus-B

Author Hershkowitz, N.; Majeski, R.; Ferron, J.; Breun, R.; Brooker, P.; Brouchous, D.; Browning, J.; Diebold, D.; Goulding, R.; Intrator, T.; Keil, D.; Meassick, S.; Nelson, B.; Persing, H.; Probert, P.; Radtke, J.; Roberts, D.;

Severn, G.; Wen, Y.

Editor(s): Ortolani, S.; Sindoni, E.

Publication Date: 1988

1988

6/6, AU, PY/17 (Item 17 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

03544019 INSPEC Abstract Number: C85051245.

Title: Research databanks-international state-of-art and experience from their constitution at the AdW of the

GDR

Author Keil, D.

Publication Date: 1985

1985

6/6, AU, PY/18 (Item 18 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

03537558 INSPEC Abstract Number: A85116798

Title: Rate constants for the reaction of hydroxyl radicals with acetaldehyde from 244-528K

Author Michael, J.V.; Keil, D.G.; Klemm, R.B.

Publication Date: 15 Aug. 1985

1985

6/6, AU, PY/19 (Item 19 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

03169397 INSPEC Abstract Number: A84010179

Title: Supercooled molecules in molecular beams of ICl and IBr

Author Keil, D.; Lubbert, A.; Schugerl, K.

Publication Date: 15 Oct. 1983

1983

6/6,AU,PY/20 (Item 20 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

02771196 INSPEC Abstract Number: A81106927

Title: Rate constants for the reaction of ground state atomic oxygen with methanol

Author Keil, D.G.; Tanzawa, T.; Skolnik, E.G.; Klemm, R.B.; Michael, J.V.

Publication Date: 15 Sept. 1981

1981

6/6, AU, PY/21 (Item 21 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

02593501 INSPEC Abstract Number: A80102538

Title: Fluorescence lifetime studies of NO/sub 2/. IV. Temperature dependence of fluorescence spectra and of

collisional quenching of fluorescence

Author Keil, D.G.; Donnelly, V.M.; Kaufman, F.

Publication Date: 15 Aug. 1980

1980

>>>W: Some display codes not found in file 583: AU

6/6, AU, PY/22 (Item 22 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

02471349 INSPEC Abstract Number: A80026001

Title: Vibrational energy transfer in thermal unimolecular systems by the diffusion cloud method.

Cyclopropane

Author Kamaratos, E.; Burkhalter, J.F.; Keil, D.G.; Rabinovitch, B.S.

Publication Date: 19 April 1979

1979

6/6, AU, PY/23 (Item 23 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

02415195 INSPEC Abstract Number: A79089701

Title: Fluorescence lifetime studies of NO/sub 2/. III. Mechanism of fluorescence quenching

Author Donnelly, V.M.; Keil, D.G.; Kaufman, F.

Publication Date: 15 July 1979

1979

6/6, AU, PY/24 (Item 24 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

01900925 INSPEC Abstract Number: A76040084

Title: Defect production in purified and nitrogen doped niobium during low temperature neutron irradiation

Author Keil, D.; Decker, W.; Diehl, J.

Publication Date: Jan. 1976

1976

6/6, AU, PY/25 (Item 25 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

01625014 INSPEC Abstract Number: A74028522, B74014150

Title: Influence of annealing treatments on residual resistivity and the field dependence of the electrical

resistance of niobium at 4.2 K

Author Keil, D.; Merbold, U.; Diehl, J.

Publication Date: March 1974

1974

6/6, AU, PY/26 (Item 26 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

01225040 INSPEC Abstract Number: B71007042

Title: Electric insulation for incore use

Author Keil, D.

Publication Date: Nov. 1970

1970

6/6, AU, PY/27 (Item 27 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

01125344 INSPEC Abstract Number: A70028724

Title: Reaction H+C/sub 2/H/sub 4/: comparison of three experimental techniques

Author Barker, J.R.; Keil, D.G.; Michael, J.V.; Osborne, D.T.

Publication Date: 15 Feb. 1970

1970

6/6, AU, PY/28 (Item 1 from file: 35) Links

Dissertation Abs Online

(c) 2007 ProQuest Info&Learning. All rights reserved.

01402971

A STUDY OF EDGE PLASMA TRAPPING INDUCED BY ION CYCLOTRON RESONANT HEATING IN AN END CELL OF THE PHAEDRUS-B TANDEM MIRROR

Author: KEIL, DOUGLAS L.

Year: 1994

6/6, AU, PY/29 (Item 2 from file: 35) Links

Dissertation Abs Online

(c) 2007 ProQuest Info&Learning. All rights reserved.

511782

THE INTER-GROUP ECONOMY OF THE NEKEMATIGI, EASTERN HIGHLANDS DISTRICT, NEW GUINEA.

Author: KEIL, DANA EDDY

Year: 1974

6/6, AU, PY/30 (Item 3 from file: 35) Links

Dissertation Abs Online

(c) 2007 ProQuest Info&Learning. All rights reserved.

483300

AN INVESTIGATION OF SOME GAS-PHASE REACTIONS OF HYDROGEN ATOMS WITH UNSATURATED HYDROCARBONS AND SOME ISOTOPIC AND MIXED ISOTOPIC VARIATIONS BY

MASS-SPECTROMETRIC DETECTION IN A DISCHARGE FLOW SYSTEM: ABSOLUTE RATE DETERMINATIONS AND MECHANISM INVESTIGATIONS.

Author: KEIL, DAVID GEORGE

Year: 1973

6/6, AU, PY/31 (Item 4 from file: 35) Links

Dissertation Abs Online

(c) 2007 ProQuest Info&Learning. All rights reserved.

477958

A RE-EVALUATION OF PECTIS (L.) SUBGENUS PECTIDOPSIS (DC.) FERNALD (COMPOSITAE:

PECTIDINAE)

Author: KEIL, DAVID JOHN

Year: 1973

6/6, AU, PY/32 (Item 1 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

03208614 Inside Conference Item ID: CN033943684

Characteristics of Combustion Synthesis Flames for Production of Silicon Carbide

KEIL, D. G.; Calcote, H. F.

Conference: American Association for Aerosol Research - Annual conference; 15th

American Association for Aerosol Research, 1996

(199610)(199610)

6/6, AU, PY/33 (Item 2 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

03185818 Inside Conference Item ID: CN033734153

"Combustion of Boron by O SUB 2/NF SUB 3/N SUB 2 Oxidizers"

Keil, D. G.; Dreizin, E. L.; Hoffman, V. K.; Calcote, H. F.

Conference: Combustion Institute; Eastern States Section; Chemical and physical processes in combustion - Fall technical meeting

Eastern States Section of the Combustion Institute, 1997

(199710)(199710)

6/6, AU, PY/34 (Item 3 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

03112736 Inside Conference Item ID: CN033003330

On the Mechanism of Boron Ignition

Keil, D. G.; Dreizin, E. L.; Felder, W.; Vicenzi, E. P.

Conference: Joint Army-Navy-NASA-Air Force Combustion Subcommittee meeting - 34th

Chemical Propulsion Information Agency, 1997

(199710)(199710)

6/6, AU, PY/35 (Item 4 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

02737493 Inside Conference Item ID: CN028530847

Profile Control of Sub-0.3 um Contact Etch Features in a Medium Density Oxide Etch Reactor

Keil, D.; Cooperberg, D.; Li, L.; Mueller, G.

Conference: Plasma processing - International symposium; 12th (Plasma processing XII)

Electrochemical Society, 1998

Editor: Mathad, G. S. (199805)

6/6, AU, PY/36 (Item 5 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

02735410 Inside Conference Item ID: CN028510014

Profile Control of Sub-0.3.mu.um Oxide Etch Features in a Medium-Density Oxide Etch Reactor

Keil, D.; Mueller, G.; Nguyen, T.; Khajehnouri, K.

Conference: Electrochemical Society - Meeting; 193rd

Electrochemical Society, 1998

(199805)(199805)

6/6, AU, PY/37 (Item 6 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

02422807 Inside Conference Item ID: CN025319478

Co-operation between regional authorities to ensure transfrontier nuclear safety

Keil, D.

Conference: Nuclear safety and local/regional democracy - European conference

Council of Europe, 1998 (199706) (199706)

6/6, AU, PY/38 (Item 7 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

02172118 Inside Conference Item ID: CN022789720

Description of a Combustion Flame for the Production of Silicon Carbide

Calcote, H. F.; Keil, D. G.

Conference: Combustion Institute: Eastern States Section - Fall technical meeting

Eastern States Section of the Combustion Institute, 1997

6/6, AU, PY/39 (Item 8 from file: 65) <u>Links</u>

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

01894229 Inside Conference Item ID: CN019583525

The waist to hip ratio in comparison with dual energy x-ray absorptiometry measures of regional fat distribution in women

Taylor, R. W.; Keil, D.; Gold, E.; Goulding, A.

Conference: Nutrition Society of New Zealand - Annual meeting; 31st

The Society, 1996 (199608)

6/6, AU, PY/40 (Item 9 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

01546462 Inside Conference Item ID: CN015354698

Combustion Synthesis of Nanosized SiC~xN~y Powders

Keil, D. G.; Calcote, H. F.; Gill, R. J.

Conference: Covalent ceramics III: science and technology of non-oxides - Symposium (Covalent ceramics 3;

Covalent ceramics three)

Pittsburgh, PA, Materials Research Society, 1996

Editor: Hepp, A. F. (19951) (19951)

6/6, AU, PY/41 (Item 10 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

01241222 Inside Conference Item ID: CN012188675

Why a Sharp Soot Threshold?

Calcote, H. F.; Keil, D. G.

Conference: Chemical and physical processes in combustion - Fall technical meeting

The Institute, 1995 (199510) (199510)

6/6, AU, PY/42 (Item 11 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

01241196 Inside Conference Item ID: CN012188419

Magnesium Coating Effects in Boron Combustion

Keil, D. G.; Dreizin, E. D.; Calcote, H. F.; Felder, W.

Conference: Chemical and physical processes in combustion - Fall technical meeting

The Institute, 1995

(199510)(199510)

6/6, AU, PY/43 (Item 12 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

00590309 Inside Conference Item ID: CN005732499

Staatliche Aufsicht Ueber Kernkraftwerke In Der Bundesrepublik Deutschland

Keil, D.

Conference: Kerntechnik '94 - Jahrestagung

Bonn, Inforum Verlags- und Verwaltungsgesellschaft, 1994

(199405)(199405)

>>>W: Some display codes not found in file 583: AU

6/6, AU, PY/44 (Item 13 from file: 65) Links

Inside Conferences

(c) 2007 BLDSC all rts. reserv. All rights reserved.

00122513 Inside Conference Item ID: CN001229126

Episiotomie versus Damm-Scheidenriss - Eine prospektive Studie

Bernard, B.; Kranzfelder, D.; Keil, D.

Conference: 49 Versammlung

Springer International, 1993 Editor: Krebs, D.; Berg, D.

(199209)(199209)

Set Items Description
S1 7 S AU=(KEIL D? OR KEIL, D? OR KEIL(2N)DEAN)
S2 4 S S1 NOT PY>1998
; show files --

[File 20] Dialog Global Reporter 1997-2007/Feb 05

(c) 2007 Dialog. All rights reserved.

[File 15] ABI/Inform(R) 1971-2007/Feb 03

(c) 2007 ProQuest Info&Learning. All rights reserved.

[File 610] Business Wire 1999-2007/Feb 05

(c) 2007 Business Wire. All rights reserved.

*File 610: File 610 now contains data from 3/99 forward. Archive data (1986-2/99) is available in File 810.

[File 810] Business Wire 1986-1999/Feb 28

(c) 1999 Business Wire. All rights reserved.

[File 476] Financial Times Fulltext 1982-2007/Feb 04

(c) 2007 Financial Times Ltd. All rights reserved.

[File 613] PR Newswire 1999-2007/Feb 05

(c) 2007 PR Newswire Association Inc. All rights reserved.

*File 613: File 613 now contains data from 5/99 forward. Archive data (1987-4/99) is available in File 813.

[File 813] PR Newswire 1987-1999/Apr 30

(c) 1999 PR Newswire Association Inc. All rights reserved.

[File 634] San Jose Mercury Jun 1985-2007/Feb 01

(c) 2007 San Jose Mercury News. All rights reserved.

[File 624] McGraw-Hill Publications 1985-2007/Feb 05

(c) 2007 McGraw-Hill Co. Inc. All rights reserved.

*File 624: Homeland Security & Defense and 9 Platt energy journals added Please see HELP NEWS624 for more

[File 9] Business & Industry(R) Jul/1994-2007/Feb 02

(c) 2007 The Gale Group. All rights reserved.

[File 275] Gale Group Computer DB(TM) 1983-2007/Feb 01

(c) 2007 The Gale Group. All rights reserved.

[File 621] Gale Group New Prod.Annou.(R) 1985-2007/Jan 26

(c) 2007 The Gale Group. All rights reserved.

[File 636] Gale Group Newsletter DB(TM) 1987-2007/Feb 01

(c) 2007 The Gale Group. All rights reserved.

[File 16] Gale Group PROMT(R) 1990-2007/Feb 01

(c) 2007 The Gale Group. All rights reserved.

[File 160] Gale Group PROMT(R) 1972-1989

(c) 1999 The Gale Group. All rights reserved.

[File 148] **Gale Group Trade & Industry DB** 1976-2007/Jan 26 (c)2007 The Gale Group. All rights reserved.

2/3,K/1 (Item 1 from file: 275) Links

Gale Group Computer DB(TM)

(c) 2007 The Gale Group. All rights reserved. 02163295 Supplier Number: 20506145

Real-time monitoring simplifies debug. (Texas Instruments' Real-Time Data Exchange, for working with

TMS320 DSPs)(Brief Article)(Product Announcement)

Keil, Deborah; Szewerenko, Lee

Electronic Engineering Times, n1003, p92(1)

April 20, 1998

Document Type: Brief Article Product Announcement

ISSN: 0192-1541

Language: English Record Type: Citation

Keil, Deborah...

2/3,K/2 (Item 2 from file: 275) <u>Links</u>

Gale Group Computer DB(TM)

(c) 2007 The Gale Group. All rights reserved. 01027732 Supplier Number: 00502493

Saving Strings.

Keil, D.M.

80 Micro, n44, p116

Sept., 1983

ISSN: 0744-7868

Language: ENGLISH F

Record Type: ABSTRACT

Keil, D.M.

2/3,K/3 (Item 1 from file: 16) Links

Gale Group PROMT(R)

(c) 2007 The Gale Group. All rights reserved.

05568340 Supplier Number: 48433261 (USE FORMAT 7 FOR FULLTEXT)

Real-time monitoring simplifies debug

Keil, Deborah; Szewerenko, Lee Electronic Engineering Times, p 92

Electronic Engineering Times , p

April 20, 1998

Language: English Record Type: Fulltext Document Type: Magazine/Journal; Trade

Word Count: 564

Keil, Deborah; Szewerenko, Lee

2/3,K/4 (Item 1 from file: 148) <u>Links</u> Gale Group Trade & Industry DB

(c)2007 The Gale Group. All rights reserved.

10127267 Supplier Number: 20506145 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Real-time monitoring simplifies debug. (Texas Instruments' Real-Time Data Exchange, for working with TMS320 DSPs) (Brief Article) (Product Announcement)

Keil, Deborah; Szewerenko, Lee

Electronic Engineering Times, n1003, p92(1)

April 20, 1998

Document Type: Brief Article Product Announcement

ISSN: 0192-1541 Language: English Record Type: Fulltext

Word Count: 604 Line Count: 00052

Keil, Deborah...

Set Items Description
S1 0 S AU=(KEIL D? OR KEIL, D? OR KEIL(2N)DEAN)
; show files

[File 256] TecInfoSource 82-2007/Aug

(c) 2007 Info. Sources Inc. All rights reserved.

[File 625] American Banker Publications 1981-2007/Feb 05

(c) 2007 American Banker. All rights reserved.

[File 268] Banking Info Source 1981-2007/Jan W4

(c) 2007 ProQuest Info&Learning. All rights reserved.

[File 626] Bond Buyer Full Text 1981-2007/Feb 05

(c) 2007 Bond Buyer. All rights reserved.

[File 267] Finance & Banking Newsletters 2007/Feb 05

(c) 2007 Dialog. All rights reserved.

[File 608] KR/T Bus.News. 1992-2007/Feb 05

(c)2007 Knight Ridder/Tribune Bus News. All rights reserved.

```
Items '
              Description
               S COMPUTER? ? OR CPU? ? OR CENTRAL() PROCESSING OR PROCESSOR? ? OR SERVER?
? OR MINICOMPUTER? ? OR MICROCOMPUTER? ? OR PC OR LAPTOP? ? OR HANDHELD? ? OR NOTEBOOK? ?
OR COMPUTING OR MAINFRAME? ? OR MAIN()(FRAME OR FRAMES) OR SYSTEM? ? OR SELF()SERVIC? OR
ATM OR ATMS OR ((AUTOMATED OR AUTOMATIC)()(TELLER OR TRANSACTION OR SERVICE) OR CASH OR
MONEY OR BANK) (W) (MACHINE? OR TERMINAL? ?) OR ELECTRONIC() TELLER? ?
               S VIRTUAL OR ONLINE OR ON()LINE OR INTERNET OR NET OR WEB OR WWW OR CYBER
OR ELECTRONIC OR WEBSITE? OR WEBPAGE? OR WEB()(SITE? OR SERVER? ?)
               ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNSPECIF? OR
UNKNOWN OR ?NO?(2N)(PERSONAL OR USER) FROM 350, 347
              S S3(5N)(DATA OR DEMOGRAPHIC? ? OR INFORMATION OR NUMBER? ? OR
IDENTIFICATION OR NAME? ? OR ID)
      1013287 S PASSWORD OR PIN OR PERSONAL()(IDENTIFICATION OR ID)()NUMBER OR CODE OR
KEY OR (PASS OR SECRET)()(WORD? ? OR PHRASE? ? OR NUMBER? ?) OR PASSPHRASE OR PASSNUMBER
OR (SECURITY OR ACCESS)()(CODE? ? OR KEY? ?) OR USER()(ID OR IDENTIFICATION OR NAME)
               S LOGON OR LOGIN OR (LOG OR LOGG? OR SIGN OR SIGNING OR SIGNED) () (IN OR
ON) OR AUTHENTICAT? OR (UNIQUE OR UNCOMMON OR DISTINGUISHING OR
DISTINCTIVE) (10N) (INFORMATION OR DATA OR STATISTIC? ? OR NUMBER? ?)
               S PATRON? ? OR CUSTOMER? ? OR CLIENT? ? OR USER? ? OR SUBSCRIBER? ? OR
ENROLEE? ? OR PARTICIPANT? ? OR PARTICIPAT?R? ? OR PERSON? ? OR DRIVER? ? OR OPERATOR? ?
(5N) GENERAT??? OR ACCOMPLISH? OR BRING() ABOUT OR CREATE? OR FORM? ? OR INITIAT?
               S TRANSACTION? ? OR ORDER? ? OR PROCEDURE? ? OR INTERACTION? ? OR DEALING?
      2502986
? OR ACTION? ? OR TRADE? ? OR TRADING OR PURCHAS??? OR EXCHANG??? OR DEAL? ? OR SELL??? OR
SALE? ? OR BUY???
               S S4(S)S5
         5582
              S S4(S)S6
         1440
S10
         2465
              S S9(S)S7
S11
              S S10(S)S7
S12
         847
              S (S11(S)S8)(S)(S1 OR S2)
          464
S13
              S (S12(S)S8)(S)(S1 OR S2)
          213
S1.4
          144 S S13 AND S14
S15
          76 S S15 AND IC=G06F
$16
          36 S S15 AND IC=G06F-017/60
S17
         3671 S S4(5N)S5
S1.8
         562 S S4 (5N) S6
S19
              S S18 AND S19
          275
S20
          159
              S S20(S)S7
S21
S22
          108
              S S20(10N)S7
              S S22(S)(S1 OR S2)
          73
S23
              S S22(10N)(S1 OR S2)
           49
S24
          3
              S S24 AND IC=G06F-017/60
S25
              S S1(3N)S3
S26
         6028
S27
            3
               S S25 (3N) S5
S28
         8990
               S S3 (5N) S5
                S S28(5N)S1
S29
         1391
                S ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNIQUE OR
       190908
S30
UNSPECIF? OR UNKNOWN OR "NO" (2N) (PERSONAL OR USER)
                S TRANSACTION? ? OR ACCOUNT? ? OR INTERACTION? ? OR ACTION? ? OR
       891326
PURCHAS??? OR DEAL? ?
                S S30(S)S31
        13891
S32
                S S32(S)S1
S33
         6303
S34
         2542
                S S30(5N)(DATA OR DEMOGRAPHIC? ? OR INFORMATION OR NUMBER? ? OR
        33257
IDENTIFICATION OR NAME? ? OR ID)
S36
          871
               S S35(5N)S31
                S S36(10N)(S1 OR S2)
S37
          371
         104 S S37(5N)S5
S38
         6313 S S35(5N)S5
S39
S40
         379 S S39(10N)S31
          179 S S40(10N)S7
S41
         131 S S41(S)S1
S42
```

```
S43
         5790
                S S35(3N)S5
S44
          230
                S S43(3N)S31
S45
          157
                S S44(S)S1
S46
           86
                S S44(10N)S1
                S S45(5N)S1
S47
          115
                S S47 AND IC=G06F-017/60
S48
                S S44 AND AU=(KEIL D? OR KEIL, D? OR KEIL(2N)DEAN)
           46
S49
           46
                IDPAT (primary/non-duplicate records only)
S50
 ; show files
```

[File 350] Derwent WPIX 1963-2006/UD=200709

(c) 2007 The Thomson Corporation. All rights reserved.

[File 347] JAPIO Dec 1976-2006/Oct(Updated 070201)

(c) 2007 JPO & JAPIO. All rights reserved.

^{*}File 350: DWPI has been enhanced to extend content and functionality of the database. For more info, visit http://www.dialog.com/dwpi/.

t s50/ti,td,ta,au,iv/all

>>>W: Some display codes not found in file 347: TD TA IV

50/TI,TD,TA,AU,IV/1 (Item 1 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0014742483

WPI Acc no: 2005-090109/

Credit card transaction system for travel agent, has verifier to compare stored code derived by decrypting digital signature with unique code obtained from transaction data and human identifier for verifying transaction

Original Titles:

Methods and apparatus for generating secure endorsed transactions

Inventor: MOVALLI B; MOVALLI M

Alerting Abstract US A1

NOVELTY - The system has an encoder to generate a unique code from an input data comprising transaction data and a human identifier. A **processor** encrypts the code using keys of an asymmetrical key pair to output a signature. A formatter formats a secure endorsed transaction using the signature and the input data. A verifier compares a stored code derived by decrypting the digital signature with the unique code to verify the transaction. DESCRIPTION - An INDEPENDENT CLAIM is also included for a method for processing secure endorsed transactions.

USE - Used for credit card transaction, in which credit card is utilized for paying for goods and services e.g. food at grocery store, clothes at department store, gas at gasoline station, airline tickets at travel agent, automobile at car dealer

ADVANTAGE - The verifier compares a stored code derived by decrypting the digital signature with the unique code to verify the transaction, thus providing a forge-resistant, tamper-resistant secure endorsed transactions. DESCRIPTION OF DRAWINGS - The drawing shows an operational flow chart of the procedure to verify the integrity of a secure endorsed transaction.

Original Publication Data by Authority

Inventor name & address:

Movalli, Michael, Manchester, MA, US, Manchester, MA, US Movalli, Brian, Lowell, MA, US, Lowell, MA, US

50/T1,TD,TA,AU,1V/2 (Item 2 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0014685633

WPI Acc no: 2005-033221/

Electronic transaction system, has card functioning on basis of pre-coding by secret number e.g. personal identification number, generated electronically with two magnetic strips

Inventor: PIAM S

Alerting Abstract FR A1

NOVELTY - The system has a card functioning on a basis of pre-coding by a secret number e.g. personal identification number, generated electronically with two magnetic strips for assuring anonymity of user in an electronic transaction on an Internet. The secret number is printed in the card and stored in a central **server** of an enterprise.

USE - Used for electronic transaction by a credit card, payment card and bank card on Internet.

ADVANTAGE - The system assures secured transaction on the Internet, thus avoids the risk of piracy of the credit card and bank card. The secret code is stored in the central server such that the card cannot be used by others, therefore the user need not worry about losing his card.

Original Publication Data by Authority

Inventor name & address: PIAM S.

50/TI,TD,TA,AU,IV/3 (Item 3 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0014649877

WPI Acc no: 2004-831896/

Merchants information providing system for use in financial transaction network, has computer system combining similar identified merchants to form ranked set, and communicating few merchants of set to user information

Original Titles:

Use of financial transaction network(s) information to generate personalized recommendations USE OF FINANCIAL TRANSACTION NETWORK(S) INFORMATION TO GENERATE PERSONALIZED RECOMMENDATIONS

UTILISATION D'INFORMATION DE RESEAU(X) DE TRANSACTIONS FINANCIERES POUR L'ELABORATION DE RECOMMANDATIONS PERSONNALISEES

Inventor: ANDRE O

Alerting Abstract US A1

NOVELTY - The system has a computer system (10) for identifying a set of merchants from a set of information selected from a group consisting of a subset of the user's payment tools transactions history, a subset of the user's

accounts transactions history, an input of reference merchants by the user. The system combines similar identified merchants to form a ranked set, and communicating few merchants of the set to user information.

USE - Used in a financial transaction network for providing information e.g. unique merchant identification code, on merchants to users of the network.

ADVANTAGE - The method facilitates the financial transaction network to automatically deepens its relationship with its user's and its affiliated merchants, and hence creating a virtuous circle in favor of the use of the payment tool.

DESCRIPTION OF DRAWINGS - The drawing shows an illustration of the overall description of an implementation of a recommendation service that operates in merchants information providing system, and represents the flows of information between the components of the system.

- 10 Computer system
- 30 Merchants information table
- 50 Web server
- 60 Customer service server
- 70 Customer service equipment

Original Publication Data by Authority

Inventor name & address:

Andre, Olivier, Liedekerke, BE, Liedekerke, BE ANDRE, Olivier, Warandestraat 167, B-1770 Liedekerke, BE, BE

50/TI,TD,TA,AU,IV/4 (Item 4 from file: 350) <u>Links</u> Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0014434211

WPI Acc no: 2004-624644/

Purchase transaction authorizing method for purchase transaction payment system, involves authorizing transaction when received confirmation code corresponds to unique transaction identification code Original Titles:

System facilitating a purchase transaction over a wireless network Inventor: TANABIAN M M; ZAHIR AZAMI B S

Alerting Abstract US A1

NOVELTY - The method involves producing a unique transaction identification code (TID) (125), upon reception of a selection request. The transaction code is encrypted by a pseudo random number generator, and a confirmation code is received from a service center (170). A transaction is authorized when the received confirmation code corresponds to the unique transaction identification code.

DESCRIPTION - An INDEPENDENT CLAIM is also included for a method for completion of a purchase transaction over a wireless network.

USE - Used for authorizing purchase transaction (claimed) in a purchase transaction payment system that is utilized for transactions with a vending machine, video rental, coffee machine, fast food, cinema, sport facility, laundry, copy machine, fax machine, Internet node, automatic photo taking machine, gas station, carwash, toll highway, bus, tramway and metro ticket seller, taxi payment, game consul, public washroom, change machine, and relaxation, massage and oxygen machine, over a wireless network.

ADVANTAGE - The method provides transaction to be completed or fulfilled without need for an explicit permanent network connection or network connectivity at the vendor site.

DESCRIPTION OF DRAWINGS - DESCRIPTION OF DRAWING - The drawing shows a block diagram illustrating preferred network layers of a data exchange methodology.

125 Unique transaction identification code

110 Vendor station

140 User

150 Mobile device

170 Service center

Original Publication Data by Authority

Inventor name & address: Zahir Azami, Bahram Seyed, Ottawa, CA, Ottawa, CA Tanabian, Mohammad M., Kanata, CA, Kanata, CA

50/T1,TD,TA,AU,IV/5 (Item 5 from file: 350) <u>Links</u> Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0014290471

WPI Acc no: 2004-477121/

Secure endorsed transaction system in grocery store, verifies integrity of secure endorsed transaction by comparing unique code derived from input data, with new code generated with endorsed transaction Original Titles:

Method and apparatus for generating secure endorsed transactions

Inventor: MOVALLI B; MOVALLI M

Alerting Abstract US B1

NOVELTY - An encoder generates unique code from input data including transaction data, identifier and two keys. A **processor** generates digital signature by encrypting unique code. A formatter formats secure endorsed transaction using digital signature and input data. Integrity of transaction is verified, by comparing unique code derived by decrypting digital signature, with a new code generated with endorsed transaction.

USE - Secure endorsed transaction system for point-of-sale equipment used in grocery store, department store, gasoline station and also used by travel agent and car dealer.

ADVANTAGE - Enables to generate secured endorsed transaction having transaction data and identifiers

corresponding to parties endorsing the transactions.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the secure endorsed transaction system. 100 secure endorsed transaction system

Original Publication Data by Authority

Inventor name & address:

Movalli, Michael, Manchester, MA, US, Manchester, MA, US Movalli, Brian, Lowell, MA, US, Lowell, MA, US

50/TI,TD,TA,AU,IV/6 (Item 6 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0014236966

WPI Acc no: 2004-422946/

Apparatus for verification of transaction to be effected by card holder, allows or refuses transaction based on comparison result of stored unique codes and codes entered by card holder at card reading machine Original Titles:

Transaction verification Inventor: HOWELL D W

Alerting Abstract GB A

NOVELTY - A server stores a list of transaction numbers for each card holder and corresponding unique codes. The card holder enters transaction number and unique code stored in a data carrier held by him to sale card reading machine which is communicably coupled to **server**, while effecting transaction at machine. The **server** compares entered and stored codes, and allows or refuses transaction based on comparison result.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 1. method for verification of transaction; and
- 2. data carrier for verification of transaction.

USE - Apparatus for verification of transaction to be effected by holder of authentication card e.g. debit card and credit card.

ADVANTAGE - Prevents fraudulent use of the authentication card, easily.

DESCRIPTION OF DRAWINGS - The figure shows the flowchart explaining the transaction verification process.

Original Publication Data by Authority

Inventor name & address:
HOWELL D W,
Howell, David William, Westcliff-on-Sea, GB, Westcliff-on-Sea, GB

50/TI,TD,TA,AU,IV/7 (Item 7 from file: 350) <u>Links</u> Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0013983458

WPI Acc no: 2004-164464/

Method for approving credit card transaction by using interactive character message

Inventor: KIM J Y

Alerting Abstract KR A

NOVELTY - A credit card transaction approval method is provided to enable a credit card member to check a credit card transaction via a mobile terminal so that it can prevent others from using the member's credit card though the credit card number is exposed or hacked.

DESCRIPTION - The method comprises several steps. A customer inputs credit card data, a mobile phone number and a secret number at an online shop for paying a commodity or a service with a credit card(1). The online shop transmits the input data to a payment gateway(2). The payment gateway transmits a transaction confirmation request message, including a callback URL, to the mobile phone by using the transmitted mobile phone number(3). The customer transmits the transaction confirmation message and the secret number to the payment gateway by using the callback URL(4). The payment gateway compares the secret number, transmitted by the online store, with that, transmitted by the customer, and if the two secret numbers are identical, transmits a transaction approval request to a credit card company(5). A server of the credit card company checks a credit state of the customer, and transmits an approval result to the payment gateway(6). The payment gateway transmits the approval result to the online store(7).

Original Publication Data by Authority

Inventor name & address: KIM J Y,

50/TI,TD,TA,AU,IV/8 (Item 8 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0013801626

WPI Acc no: 2003-901732/

Online/real-time editing method for cellular telephone, involves searching order data file and displaying searched file to user for editing and forwarding to buyer

Original Titles:

Method and system for online and feal-time editing and forwarding manifestsza

Inventor: CHIEN S; CHU T; LEE Y; WU K

Alerting Abstract US A1

NOVELTY - An order data file (32) is searched in the database server through a searching module (42) based on the input identification code of order file. The searched file is displayed to the user through the terminal (2) for online and real-time editing. The edited file is forwarded to the buyer who makes purchase order, based on the edited data. DESCRIPTION - An INDEPENDENT CLAIM is also included for system for online/real-time editing and forwarding of data.

USE - For online and real-time editing of order data file using cellular phones and desktop personal computer. ADVANTAGE - Transaction cost is reduced and market situation is controlled in real-time.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of online/real-time editing process.

2 terminal

32 order data file

42 searching module

44 editing module

46 delivery module

Original Publication Data by Authority

Inventor name & address: Chu, Te-Mei, Taipei, TW, Taipei, TW Chien, Shu-Mei, Taipei, TW, Taipei, TW Lee, Yun-Chi, Taipei, TW, Taipei, TW Wu, Kuan-I, Taipei, TW, Taipei, TW

50/TI,TD,TA,AU,IV/9 (Item 9 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0013706391

WPI Acc no: 2003-803550/

Electronic payroll and work management system for labor intensive industries, compares employee account and personal identification numbers with prestored numbers, to authenticate employee for providing check in/out status

Original Titles:

Multi-purpose terminal, payroll and work management system and related methods Multi-purpose terminal, payroll and work management system and related methods Inventor: BEN-AISSA N

Alerting Abstract US Al

NOVELTY - A computer in communication with automatic teller machine (ATM)-payroll and work management (APW) terminal (20), compares unique identification (ID) account number and personal ID number read by terminal from APW card (23), with number prestored in memory. When the numbers corresponds, the employee account number is authenticated and provides current time as payroll check-in/check-out status of respective employee. DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 3. electronic payroll processing method; and
- 4. ATM-payroll-work management electronic terminal.

USE - Automatic teller machine-payroll-work management (APW) system for labor-intensive industries such as janitorial services and fast food franchises.

ADVANTAGE - The employee payrolls are processed within short time period, thereby paying the employees immediately. Also minimizes the payroll frauds and expense.

DESCRIPTION OF DRAWINGS - The figure shows a top plan view of the APW electronic payroll system.

20 APW terminal

21 display screen

22 slot

23 APW card

30-34 keys

Original Publication Data by Authority

Inventor name & address:

Ben-Aissa, Nebil, Palatine, IL, US, Palatine, IL, US Ben-Aissa, Nebil, Palatine, IL, US, Palatine, IL, US

50/T1, TD, TA, AU, IV/10 (Item 10 from file: 350) Links

Derwent WPIX -

(c) 2007 The Thomson Corporation. All rights reserved:

0013550648,

WPI Acc no: 2003-644553/

Check transaction processing system for grocery store, retrieves customer record storing check verification status information, from database using customer identification code in response to request from transaction terminal

Original Titles:

SYSTEM, METHOD, AND DATABASE FOR PROCESSING TRANSACTIONS

Inventor: DEATON D W

Alerting Abstract US Al

NOVELTY - The system has a transaction terminal connected to a transaction processor which maintains customer information including check verification status in a database. The processor retrieves the customer record from the database using a customer identification code (ID), in response to the customer request received from the terminals. An appropriate response is transmitted based on retrieved record or lack of customer record.

DESCRIPTION - An INDEPENDENT CLAIM is also included for check verification method.

USE - For processing transactions of multiple-store business e.g. grocery stores.

ADVANTAGE - The store's marketing and other customer relation programs are improved by maintaining the transaction data and customer profiles. The customer information is collected in an unobtrusive and efficient manner during high volume check transactions.

DESCRIPTION OF DRAWINGS - The figure shows a flowchart illustrating the check verification method.

Original Publication Data by Authority

Inventor name & address: DEATON, DAVID W., ABILENE, TX, US, ABILENE, TX, US

50/T1,TD,TA,AU,1V/11 (Item 11 from file: 350) <u>Links</u> Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0013420798

WPI Acc no: 2003-511353/

Unified electronic payment system

Inventor: KIM S J

Alerting Abstract KR A

NOVELTY - A unified electronic payment system is provided to secure a safe transaction between a purchaser and a seller though not using stores affiliated at a conventional credit card company.

DESCRIPTION - The system comprises several steps. A seller or a purchaser accesses a credit card host system, and requests the host system to open a virtual affiliated store(s100). The host system allows the virtual affiliated store to be opened(s110). The purchaser makes payment for a commodity at the virtual affiliated store by using a credit card(s120). The host system notifies the purchaser or the seller of the opening of the virtual affiliated store, then the purchaser or the seller notifies the other side of the opening of the virtual affiliated store, and the purchaser transmits the credit number and the secret number to the host system. The host system processes the credit card payment by using the credit card number and the secret number, and transmits the process result to the purchaser

and the seller(s130).

Original Publication Data by Authority

Inventor name & address: KIM S J.

50/TI,TD,TA,AU,IV/12 (Item 12 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0013234675

WPI Acc no: 2003-319770/

Software license management system, verifies purchaser's unique identification code and secret key using software license information in server before transmitting software

Original Titles:

SOFTWARE LICENSE MANAGEMENT SYSTEM

Inventor: ANEGAWA T; ISHIDAIRA I

Alerting Abstract JP A

NOVELTY - A software database (6) and a license management database (7) in a server (2) register the software for marketing and software license information of each software purchaser respectively. The server transmits the software to any of the purchaser terminals (3a-3c) through a communication circuit (1) after verifying purchaser's unique ID code and secret key using the software license information.

USE - For managing software license through communication circuit such as Internet.

ADVANTAGE - Since the information are transmitted after authenticating the purchaser, the software being irregularly installed in personal computers other than the software purchaser is prevented efficiently.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the software license management system. (Drawing includes non-English language text).

1 communication circuit

2server

3a-3cpurchase terminals

6software database

7license management database

Original Publication Data by Authority

Inventor name & address: ANEGAWA TAKEHIKO,

ISHIDAIRA IKU,

50/TI,TD,TA,AU,IV/13 (Item 13 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0013083716

WPI Acc no: 2003-164307/

System and method for making payment by using bank account of payment postponement

Inventor: RABH

Alerting Abstract KR A

NOVELTY - A payment system and method is provided to enable a buyer to place a purchase order and at the same time, make payment by using a transfer from a buyer's account to a seller's account, a payment postponement account from which the seller can not withdraw a money for a period so that it makes it easy for the buyer to request a repayment, a settlement or a payment suspension in a case that a delivered commodity or a service is abnormal. DESCRIPTION - The method comprises steps of a buyer searching for a desired commodity in an electronic commerce site, transmitting a purchase order for a searched commodity to the electronic commerce site, and making payment for the purchased commodity(401), the site displaying order specifications and offering a web window for enabling the buyer to input the buyer data, delivery destination data and a payment method(402), a buyer terminal transmitting the buyer data, the destination data and seller data to an account payment server if the buyer selects an account payment method(403), the account payment server extracting the name of the site and an account number, and transmitting a web page for inputting a buyer ID and an account secret number to the buyer terminal (404), the buyer inputting the buyer ID and the account secret number on the web page, and the account payment server checking a balance of the account (405), the account payment server transferring the purchase price from the buyer account to the electronic commerce site account which is a payment postponement account (406), the account payment server transmitting an account transfer process result to the buyer terminal (407), the account payment server transmitting ordered data to the site(408), the buyer requesting a repayment to the account payment server if a delivered commodity is abnormal(410), the account payment server requesting detailed data to the site(411), the site transmitting the requested detailed data to the account payment server (412), the account payment server taking a repayment, a settlement or a payment suspension based on the collected data(413), and the account payment server transmitting a taken action to the buyer via an e-mail(414).

Original Publication Data by Authority

Inventor name & address: RA B H.

50/TI,TD,TA,AU,IV/14 (Item 14 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0013057080

WPI Acc no: 2003-136795/

Credit transaction system using bar code

Inventor: KIM J H; KIM K J; LEE S D; SOHN J H

Alerting Abstract KR A

NOVELTY - A credit transaction system is provided to register at a portable terminal a bar code with conventional credit card data and a secret number, and to display the bar code on the portable terminal according to a request of a user when the user wants to purchase a commodity or a service.

DESCRIPTION - The system comprises a portable terminal(200) and a financial institute. The portable terminal(200) includes a data input unit(201), a bar code storage(202), a secret number storage(203), a display(204), a cable connector(205) and a CPU(206). The data input module(201) enables a user to input a secret number, a bank name and an account number. The bar code storage(202) stores a bar code issued for the user. The secret number storage(203) stores secret numbers corresponding to bar codes. The display(204) displays the bar code according to a request of the user. The cable connector(205) connects the portable terminal to a server of a bank for downloading a new bar code. The CPU(206) controls the bar code storage operation of the bar code storage(202), analyzes the input data, i.e. a bank name and a secret number, extracts the bar code from the bar code storage(202) based on the analysis result, and controls the display of the extracted bar code. If a user wants to receive a new bar code from a bank, the user visits the bank, fills in an application form, and offers a portable terminal to the bank. Then the bank checks a credit state of the user and determines an issue of the bar code according to the credit state. If the credit state of the user is normal, the bank downloads the bar code to the portable terminal via the cable connector(205).

Original Publication Data by Authority

Inventor name & address: KIM J H, KIM K J, LEE S D, SOHN J H,

50/TI,TD,TA,AU,IV/15 (Item 15 from file: 350) <u>Links</u> Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0012962951

WPI Acc no: 2003-040059/

User authentication system for Internet-based financial transactions, compares unique user identification information stored in CD with input password of user, for authenticating user

Original Titles:

System, process and article for conducting authenticated transactions

Inventor: FISHMAN J M; POWERS L

Alerting Abstract US A1

NOVELTY - A server (30) receives the unique user identification information stored in a CD (11) and a password input by a user. The server authenticates the user for transaction, when the stored information matches with the input password.

DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

- 5. User authentication method; and
- 6. Wallet-sized optical storage medium storing user authentication program.

USE - For authenticating user in Internet-based financial transactions.

ADVANTAGE - Since the user is authenticated only after matching the password with the information stored in the CD, additional level of security is provided.

DESCRIPTION OF DRAWINGS - The figure shows a schematic view of the user authentication system.

11 CD

30 Server

Original Publication Data by Authority

Inventor name & address:

Fishman, Jayme Matthew, North Reading, MA, US, North Reading, MA, US Powers, Larry, Encinitas, CA, US, Encinitas, CA, US

50/TI,TD,TA,AU,IV/16 (Item 16 from file: 350) <u>Links</u>

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012926051

WPI Acc no: 2003-002543/

Commercial transaction using prepayment card over the Internet, uses personal computer or mobile phone, certification center validates data contained on prepayment card

Alerting Abstract FR A1

NOVELTY - Method has stages as follows:

A. establish connection between the sale site and certification center; collect and send number series and associated secret code to certification center; verify validity of number and code; verify credit on prepaid card; send payment authorization from certification center to sale site if verification of code and credit is positive; notify user of purchase validation.

DESCRIPTION - Uses prepaid card having number series and associated secret code, to purchase service or object from sale site to which user has access via at least a partially public network. In second stage the connection to certification center is done automatically as son as the user selects the payment mode by prepaid card. The number series is composed of at least 10 alphanumeric characters and the secret code has at least 16 alphanumeric characters. In the first and last stages the data is transmitted in encrypted format. The user can access the sale site via a mobile phone via the certification center. The second stage is repeated a predetermined number of times in case of negative verification of number and code. An Independent Claim is also included for a prepaid card payment system

USE - For making purchases over the Internet using prepayment cards.

ADVANTAGE - Simple system which allows a user to makes remote purchase, even for small cost amounts, and guaranteeing risk limitation in case of fraud and complete confidentiality at moment of payment.

DESCRIPTION OF DRAWINGS - The drawing illustrates a global view of the system

2 personal computer

3 mobile phone

4 data processing and storage center

5 server

7 banks server

- 41 prepayment cards authentication and management server
- 42 database

43 second server.

50/TI,TD,TA,AU,IV/17 (Item 17 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012880931

WPI Acc no: 2002-740218/

Action verification method e.g. for financial transaction in bank, involves comparing PIN and individual accounts included in verification request, with corresponding stored information, to verify requested action Original Titles:

Action verification system using central verification authority Action verification system using central verification authority

Inventor: TALKER A I

Alerting Abstract US A1

NOVELTY - The prestored personal identification numbers (PINs) and the accounts of individual or organization (14) are compared with corresponding information included in a verification request (22), requesting a verification of the action. The action is verified when the identification number and the accounts match, and the verification result (23) is transmitted to the requesting party (12).

DESCRIPTION - An INDEPENDENT CLAIM is included for personal identity verification method.

USE - For verifying actions such as financial transaction, message, command, non-financial transaction, approval, identification request, data transmission, etc., for protecting against credit card and cheque frauds in bank, etc. ADVANTAGE - By verifying the actions, unauthorized actions are prevented, thus provides safe communication

through unprotected communication lines.

DESCRIPTION OF DRAWINGS - The figure shows a schematic block diagram of the action verification system.

- 12 Requesting party
- 14 Organization
- 22 Verification request
- 23 Verification result

Original Publication Data by Authority

Inventor name & address:

Talker, Albert Israel, Marlboro, NJ, US, Marlboro, NJ, US
Talker, Albert Israel, 14 Castlehill Dr., Marlboro, NJ 07746, US, Marlboro, NJ, US

50/TI,TD,TA,AU,IV/18 (Item 18 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012863596

WPI Acc no: 2002-722488/

Display implementation method for on-line electronic trading exchange, involves identifying all offers to sell according to trading relationship between two member accounts

Original Titles:

Trading system with anonymous rating of participants

Inventor: NICOLAISEN R A; TORMEY B P

Alerting Abstract US A1

NOVELTY - The default payment terms and the trading relationship between two member accounts are defined. An electronic trading exchange that includes at least one offer to sell is selected. A table is viewed and all offers to sell are identified according to the trading relationship.

DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

- 7. Data analysis and dissemination provision method; and
- 8. Computer system.

USE - For implementing display for on-line electronic trading exchange.

ADVANTAGE - Maintains the secrecy of identities of both the buyers and sellers and helps to preserve the integrity of the trading environment.

DESCRIPTION OF DRAWINGS - The figure shows a flowchart illustrating the operation for the accumulation and display of data on an electronic trading exchange.

Original Publication Data by Authority

Inventor name & address:

Nicolaisen, Royce Arne, Orinda, CA, US, Orinda, CA, US Tormey, Brian Patrick, Carmichael, CA, US, Carmichael, CA, US

50/TI,TD,TA,AU,IV/19 (Item 19 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012794142

WPI Acc no: 2002-649943/

Integrated circuit card issue method for online transactions, involves collecting secret key and electronic certificate data based on received issue request and accordingly card is published and dispatched Original Titles:

METHOD AND SYSTEM FOR ISSUING AND DISTRIBUTING IC CARD USED BY PKI SYSTEM

Inventor: ONISHI H

Alerting Abstract JP A

NOVELTY - A card issue request is forwarded to IC card issue terminal (30) based on the received purchase order request. The secret key and electronic certificate information generated by authentication system are collected by the issue terminal. Based on the collected information, the card is published and dispatched to relevant user through dispatch terminal (40).

DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

- 9. IC card circulation method;
- 10. IC card: and
- 11. IC card circulation system.

USE - For issue of IC card used in online transactions through internet.

ADVANTAGE - Simplifies IC card issuing due to sequential operation of service terminals with relevant data security.

DESCRIPTION OF DRAWINGS - The figure shows an outline of IC card issue system. (Drawing includes non-English language text).

30 IC card issue terminal

40 Dispatch terminal

Original Publication Data by Authority

Inventor name & address: ONISHI HIDEAKI,

50/T1,TD,TA,AU,IV/20 (Item 20 from file: 350) Links Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0012650491

WPI Acc no: 2002-499896/

Managing accounts on Internet server by using unique identification code for account access data **Original Titles:**

NETWORK ORIENTED PAYMENT SERVICE SYSTEME DE PAIEMENT ORIENTE RESEAU

Inventor: MARCOVICI M

Alerting Abstract WO Al

NOVELTY - Method consists in sending a request to the server, establishing the account access data, assigning an amount to the accounts and transmitting the access data from the server to the requesting party over the Internet. A ticket is issued with the account access data which includes an activation time and a debit access code that is verified in transactions for account debiting.

DESCRIPTION - There is an INDEPENDENT CLAIM for an Internet accounts management server.

USE - Method is for managing accounts on an Internet server.

ADVANTAGE - Method avoids transaction fees, ensures anonymity and enables transactions to be traced back to the benefiting person or organization.

DESCRIPTION OF DRAWINGS - The figure shows a payment transacted between two tickets.

Original Publication Data by Authority

Australia

Publication No. AU 200079140 A (Update 200254 E)

Publication Date: 20020415

Assignee: QENTIS HOLDING GMBH; AT (QENT-N)

Language: EN

Application: AU 200079140 A 20001005 (Local application)

WO 2000EP9723 A 20001005 (PCT Application)

Related Publication: WO 2002029740 A (Based on OPI patent)

Inventor name & address:

MARCOVICI, Michael, Farbergasse 3/8, A-101 Wien, AT, AT

50/T1,TD,TA,AU,IV/21 (Item 21 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012628683

WPI Acc no: 2002-477442/

Purchase information grasp system has analysis section to analyze purchase information based on unique bar code information along with concerned purchaser information stored in data file

Original Titles:

PURCHASE COMPREHENDING SYSTEM AND PURCHASE COMPREHENDING METHOD

Inventor: KAGOSHIMA H; NATORI H; ONUMA K; SHINTO T; TSUCHIDA I

Alerting Abstract JP A

NOVELTY - A receiver (34) receives the unique bar code information with concerned purchaser information. A data file (33) stores the information received from the receiver. An analysis section analyze the purchase information, based on unique bar code information with concerned purchaser information stored in the data file. DESCRIPTION - An INDEPENDENT CLAIM is included for purchase information grasp method.

USE - For grasping purchase information on consumer's goods to concerned goods.

ADVANTAGE - Enables confirming purchase situation of goods easily, thus versatility is improved sufficiently. DESCRIPTION OF DRAWINGS - The figure shows a block diagram of purchase information grasp system. (Drawing includes non-English language text).

33 Data file

34 Receiver

Original Publication Data by Authority

Inventor name & address: NATORI HITOSHI, ONUMA KATSUO, SHINTO TARO, KAGOSHIMA HIROSHI, TSUCHIDA ISAO.

50/TI,TD,TA,AU,IV/22 (Item 22 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012622500

WPI Acc no: 2002-471036/

Biometric data collection and transmission apparatus has biometric template generator which is connected to sensor, to convert biometric data into biometric template

Original Titles:

VERFAHREN UND VORRICHTUNG ZUM SICHEREN UBERTRAGEN UND AUTHENTISIEREN BIOMETRISCHER DATEN UBER EIN NETZWERK

METHOD AND APPARATUS FOR SECURELY TRANSMITTING AND AUTHENTICATING BIOMETRIC DATA OVER A NETWORK

PROCEDE ET APPAREIL D'EMISSION ET D'AUTHENTIFICATION SECURISEES DE DONNEES BIOMETRIQUES VIA UN RESEAU

Method and apparatus for securely transmitting and authenticating biometric data over a network METHOD AND APPARATUS FOR SECURELY TRANSMITTING AND AUTHENTICATING BIOMETRIC DATA OVER A NETWORK

PROCEDE ET APPAREIL D'EMISSION ET D'AUTHENTIFICATION SECURISEES DE DONNEES BIOMETRIQUES VIA UN RESEAU

Inventor: GLASS R W

Alerting Abstract US A1

NOVELTY - A sensor connected to a biometric template generator (105) collects biometric data. An image processor (104) connected between the sensor and the biometric template generator determines whether biometric data is suitable for template generation. The biometric template generator converts the biometric data into biometric template (105a).

DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

- 12. Cryptographic system;
- 13. Security providing method; and
- 14. Biometric information exchanging method.

USE - For collecting and transmitting biometric data used for verification of individual identity in iris system and fingerprint system used for online banking and Internet commerce transaction.

ADVANTAGE - The token defines a unique transaction and couples biometric data to the transaction, thus preventing use of biometric data at a later time or setting a time limit when the data becomes invalid. The system provides secure transmission and subsequent authentication of biometric data.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the biometric identification system.

104 Image processor 105 Biometric generator 105a Biometric template

Original Publication Data by Authority

Australia

Publication No. AU 2002365086 A1 (Update 200428 E)

Publication Date: 20030709

Assignee: IRIDIAN TECHNOLOGIES INC (IRID-N)

Inventor: GLASS R W

Language: EN

Application: AU 2002365086 A 20021021 (Local application)

Priority: US 200120791 A 20011030

Related Publication: WO 2003053123 A (Based on OPI patent)

Publication No. AU 2002365086 A8 (Update 200624 E)

Publication Date: 20051027

Assignee: IRIDIAN TECHNOLOGIES INC (IRID-N)

Inventor: GLASS R W

Language: EN

Application: AU 2002365086 A 20021021 (Local application)

Priority: US 200120791 A 20011030

Related Publication: WO 2003053123 A (Based on OPI patent)

Original IPC: G06F-11/30(A) G06F-12/14(B) G06F-17/60(B) H04K-1/00(B) H04L-9/00(B) H04L-9/32(B)

H04N-7/167(B)

Current IPC: G06F-11/30(A) G06F-12/14(B) G06F-17/60(B) H04K-1/00(B) H04L-9/00(B) H04L-9/32(B)

H04N-7/167(B)

Inventor name & address:

GLASS R W, GLASS R W,

GLASS, Randal, W., 108 Highgate Lane, Cherry Hill, NJ 08003, US, Cherry Hill, NJ 08003, US

Glass, Randal W., Cherry Hill, NJ, US, Cherry Hill, NJ, US

GLASS, Randal, W., 108 Highgate Lane, Cherry Hill, NJ 08003, US, US

50/TI,TD,TA,AU,IV/23 (Item 23 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0012509934

WPI Acc no: 2002-458088/

Goods purchase authentication system includes server to judge whether bar code data allocated for each goods is legitimate data

Original Titles:

PURCHASE CERTIFYING SYSTEM AND PURCHASE CERTIFYING METHOD

Inventor: KAGOSHIMA H; NATORI H; SHIIO I; SHINTO T; TAMURA K

Alerting Abstract JP A

NOVELTY - A bar code reader (1) inputs the unique bar code data for each goods purchased by a client (2). A CPU (21) transmits the bar code data to a server (3) through a network (4) and a database (33) stores the bar code data. The server judges whether the stored data is a legitimate data.

DESCRIPTION - An INDEPENDENT CLAIM is included for goods purchase authentication method.

USE - Goods purchase authentication system.

ADVANTAGE - Versatility of the goods purchase authentication system is improved.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the goods purchase authentication system. (Drawing includes non-English language text).

1Bar code reader

2Client

3Server

4Network

21CPU

33Database

Original Publication Data by Authority

Inventor name & address: SHIIO ICHIRO, NATORI HITOSHI, TAMURA KEIICHI, SHINTO TARO, KAGOSHIMA HIROSHI,

50/TI,TD,TA,AU,IV/24 (Item 24 from file: 350) <u>Links</u> Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0012322469

WPI Acc no: 2002-264259/

Credit guarantee method in electronic commerce, involves sending transaction proof request telegraph message including bill number to authentication server, when transaction completion message is received Original Titles:

CREDIT GUARANTEE METHOD IN ELECTRONIC COMMERCIAL TRANSACTION, AND DEALING AUTHENTICATING SERVER, STORE SERVER, AND MEMBER MANAGING SERVER APPLYING THE SAME METHOD

Method of credit guarantee in electronic commerce

Inventor: KOBAYASHI T

Alerting Abstract JP A

NOVELTY - A transaction report telegraph message containing bill number, is received by authentication server (20c) from payment system connected to user (10). A store server (20b) connected to goods selling system, sends transaction proof request telegraph message including bill number to server (20c), when transaction is completed. The server (20c) compares and records the bill numbers in telegraph messages.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- B. Transaction authentication server;
- C. Store server;
- D. Management server

USE - In electronic commerce.

ADVANTAGE - Since bill numbers from both the payment system and goods selling system are compared, forged transaction is prevented.

DESCRIPTION OF DRAWINGS - The figure shows the schematic diagram of transmission and reception of information during electronic commerce. (Drawing includes non-English language text).

10 User

20b Store server

20c Authentication server

Original Publication Data by Authority

Inventor name & address: KOBAYASHI TOSHIAKI, Kobayashi, Toshiaki, Nagano-ken, JP, Nagano-ken, JP

50/TI,TD,TA,AU,IV/25 (Item 25 from file: 350) <u>Links</u> Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0012274733

WPI Acc no: 2002-215396/

Debit account establishing system for credit card transaction, sends unique personal identifier number corresponding to debit account number in readable format from server to customer, based on received funds Original Titles:

Original littles:

System and method for debit account transactions

Inventor: KEIL D S

Alerting Abstract US A1

NOVELTY - A transaction terminal initiates point of sale transaction to accept input funds to be deposited into debit account from a customer. The terminal transmits input value of funds to host server which in turn sends unique personal identifier number (PIN) corresponding to debit account number in a readable format to the customer. DESCRIPTION - An INDEPENDENT CLAIM is also included for debit account establishment method. USE - For establishing debit account for credit card ATM, bank card, prepaid cards transaction. ADVANTAGE - Allows customer to establish debit accounts in easy and efficient manner, without providing personal identification data, thereby assuring anonymity of account. Since the system does not require the standard POS payment implements such as plastic card, smart card, etc., outlay of capital customer is minimized, and possibility of theft of card is eliminated.

DESCRIPTION OF DRAWINGS - The figure shows the transaction and funds flow of debit account establishing system.

Original Publication Data by Authority

Inventor name & address:

Keil, Dean S., Lake Worth, FL, US, Lake Worth, FL, US

50/TI,TD,TA,AU,IV/26 (Item 26 from file: 350) <u>Links</u> Derwent WPIX (c) 2007 The Thomson Corporation. All rights reserved.

0012274731

WPI Acc no: 2002-215394/

Debit account establishing apparatus for credit card transaction, sends receipt printed with personal identifier and debit account numbers to transaction terminal, depending on received funds from customer Original Titles:

Apparatus for establishing debit accounts

Inventor: KEIL D S

Alerting Abstract US A1

NOVELTY - A transaction terminal initiates point of sale (POS) transaction to accept an input value representing

funds to be deposited into debit account, from a customer. The terminal transmits input value to host which in turn sends receipt printed with personal identifier number (PIN) and debit account number, to the customer.

USE - For establishing debit account through point-of-sale (POS) terminal for credit card, bank card, ATM debit pre-paid cards transactions, etc.

ADVANTAGE - Allows customers to establish debit accounts in easy and efficient manner, without providing personal identification data, thereby assuring anonymity of account. The system does not require standard POS payment implements such as plastic card, smart card, etc., outlay of capital of customer is minimized and possibility of theft of card is eliminated.

DESCRIPTION OF DRAWINGS - The figure shows a block diagram of POS transaction terminal.

Original Publication Data by Authority

Inventor name & address:

Keil, Dean S., Lake Worth, FL, US, Lake Worth, FL, US

50/TI,TD,TA,AU,IV/27 (Item 27 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0011240292

WPI Acc no: 2002-179936/

Electronic payment system on Internet for eliminating need to supply consumer card information to shopping mall by setting electronic payment engine with form-analyzing robot

Original Titles:

Electronic payment system on internet and method the same

ELECTRONIC PAYMENT SYSTEM ON INTERNET AND METHOD THE SAME

SYSTEME DE PAIEMENT ELECTRONIQUE SUR L'INTERNET ET PROCEDE ASSOCIE

Inventor: KIM G C; KIM K

Alerting Abstract WO Al

NOVELTY - A client server (12) performs communications through the Internet (10) and includes an electronic payment program and an electronic payment engine (22) with a form-analyzing robot (23), while an electronic authentication engine (20) is connected to a financial company server (16).

DESCRIPTION - The robot analyzes a form comprising a settlement screen downloaded on the client system and extracts a settled amount of money and fields required to be input through analysis. The authentication engine issues a secret number of an account code.

AN INDEPENDENT CLAIM is included for an electronic payment method.

USE - Making electronic payments on the Internet.

ADVANTAGE - Improved security by preventing retailers obtaining customer card information.

DESCRIPTION OF DRAWINGS - The drawing shows the system

12 Client system

22 Payment engine

23 Form-analyzing robot

20 Authentication engine

16 Company server

Original Publication Data by Authority

Australia

Publication No. AU 200160768 A (Update 200236 E)

Publication Date: 20020205 Assignee: KIM K; KR (KIMK-I)

Language: EN

Application: AU 200160768 A 20010529 (Local application)

Priority: KR 200039210 A 20000710

Related Publication: WO 2002008988 A (Based on OPI patent)

Inventor name & address:

KIM G C, KIM G C,

Kim, Kwang-Chul, Busan, KR, Busan, KR

KIM, Kwang-Chul, 110-501 LG Apt., 1398 Jwa-dong, Haeundae-gu, Busan 612-768, KR, KR

50/TI,TD,TA,AU,IV/28 (Item 28 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0011166800

WPI Acc no: 2002-104341/

Method for approving credit card transaction using bidirectional text message of wireless internet

Inventor: KIM J Y

Alerting Abstract KR A

NOVELTY - A method for approving credit card transaction using a bidirectional text message of the wireless Internet is provided to prevent a credit card from piracy, by making the credit card transaction checked via a mobile communication terminal of a credit card owner in response to an identification request of a credit card company. DESCRIPTION - A credit card member registers a cellular phone number for receiving a text message in a server of a credit card company(S210). The credit card member suggests a credit card, and then requests an approval of the credit card to an approval relay company server in transaction(S220). The approval relay company server requests a

transaction approval to a credit card company, and the credit card company sends an identification message of the transaction approval request(S230). The credit card member inputs a **secret number** into a **server** of the credit card company in order to confirm the **transaction**(S240). The credit card company **server** checks the **secret number** from the credit card member, and sends resultant data of the transaction approval request to the approval relay company **server**(S250).

Original Publication Data by Authority

Inventor name & address: KIM J Y,

50/TI,TD,TA,AU,IV/29 (Item 29 from file: 350) Links Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0011011794

WPI Acc no: 2001-637225/

Method for automatically filling up order sheet using contents ordered by user

Inventor: CHO S U; KIM J G; KONG G T; LEE J W

Alerting Abstract KR A

NOVELTY - A method for automatically filling up an order sheet using contents ordered by a user is provided to embody an order filling up method and a recording medium capable of being read by a computer recording a program for implementing the method for a later ordering and a convenience of related process by using an E-mail address and a secret number inputted at ordering of an internet shopping mall user in an internet electronic commercial transaction.

DESCRIPTION - An internet electronic commercial transaction server is selected ordering information(name, E-mail address, telephone, address), delivery information(receiver and address of the receiver) and paying information(paying method, for example, non-bankbook depositing or a credit card) from an initial ordering user through an internet. Also, the internet electronic commercial **transaction** server receives a **secret number** capable of managing the user's account(201(similar)203) and stores the **secret number** in the database. As the ID, an E-mail address is used. In detail, the user selects a paying method(non-bankbook depositing or a credit card). If the user wants to pay by a non-bankbook depositing, the internet electronic commercial transaction server receives bank information to be deposited and a **secret number**. If the user wants to pay by a credit card, a **secret number** is inputted after a credit card is approved by receiving credit card information(203).

Original Publication Data by Authority

Inventor name & address:

CHO S U, KIM J G, KONG G T, LEE J W,

50/T1,TD,TA,AU,IV/30 (Item 30 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0011000652

WPI Acc no: 2001-625823/

Enabling anonymous credit transactions for the purchase of good and services from merchants over e.g. the internet

Original Titles:

Systems and methods enabling anonymous credit transactions
Systems and methods enabling anonymous credit transactions
SYSTEMS AND METHODS ENABLING ANONYMOUS CREDIT TRANSACTIONS
SYSTEMES ET PROCEDES PERMETTANT D'EFFECTUER DES TRANSACTIONS DE CREDIT ANONYMES

Inventor: BRODY R M; KENNEDY R S

Alerting Abstract WO A2

NOVELTY - Blocks of consumer credit card numbers are used to create dynamic mappings of the card numbers to account numbers or even other card numbers, e.g. pseudo-random credit card numbers. Because pseudo-random attributes are transmitted to the merchant; the transaction between the consumer and merchant will be anonymous. USE - Enables consumers to purchase goods and services from merchants, using credit cards.

ADVANTAGE - Consumers can maintain the confidentiality of their credit card numbers and identity without disclosure to the merchants.

DESCRIPTION OF DRAWINGS - The drawing shows a schematic diagram of the system employing the method.

Original Publication Data by Authority

Australia

Publication No. AU 2001239945 A8 (Update 200612 E)

Publication Date: 20051006

Systems and methods enabling anonymous credit transactions

Assignee: E-SCORING INC (ESCO-N)

Inventor: KENNEDY R S

BRODY R M Language: EN

Application: AU 2001239945 A 20010228 (Local application)

Priority: US 2000186166 P 20000229

Related Publication: WO 2001065502 A (Based on OPI patent)

Original IPC: G07F-7/10(A) G07F-19/00(B) Current IPC: G07F-7/10(A) G07F-19/00(B)

Publication No. AU 200139945 A (Update 200204 E)

Publication Date: 20010912

Assignee: E-SCORING INC; US (ESCO-N)

Language: EN

Application: AU 200139945 A 20010228 (Local application)

Priority: US 2000186166 P 20000229

Related Publication: WO 2001065502 A (Based on OPI patent)

Inventor name & address:

KENNEDY R S, BRODY R M,

Brody, Robert M., Weston, CT, US, Weston, CT, US Kennedy, Reuben S., Duluth, GA, US, Duluth, GA, US

BRODY, Robert, M., 15 Marshall Lane, Weston, CT 06897, US, US KENNEDY, Reuben, S., 590 Hilltop Lane, Duluth, GA 30136, US, US

50/TI,TD,TA,AU,IV/31 (Item 31 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0010986255

WPI Acc no: 2001-610932/

Authenticating method of products for sale over Internet for manufacturers, involves communicating unique code associated with purchase product to authenticating server for determining authenticity of product Original Titles:

SYSTEM UND VERFAHREN ZUM VERIFIZIEREN DER AUTHENTIZITAT VON PRODUKTEN MIT HILFE EINES NETZWERKS

SYSTEM AND METHOD FOR VERIFYING AUTHENTICITY OF PRODUCTS USING NETWORKS SYSTEME ET PROCEDE PERMETTANT DE VERIFIER L'AUTHENTICITE DE PRODUITS VIA DES RESEAUX

SYSTEM AND METHOD FOR VERIFYING AUTHENTICITY OF PRODUCTS USING NETWORKS SYSTEME ET PROCEDE PERMETTANT DE VERIFIER L'AUTHENTICITE DE PRODUITS VIA DES RESEAUX

Inventor: DERBYSHIRE R; DOLJACK F A; NICELY M C

Alerting Abstract WO A2

NOVELTY - A product with unique identification code is purchased over the network. On receipt of product, identification code of product is analyzed and communicated to authentication server (62) that determines whether a code is valid and whether product is authentic. This determined validity is communicated to the purchaser (58). DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- E. Sales transaction authenticating system;
- F. Database structure for use in authenticating identification indicia of products;
- G. Computer data transmission system;
- H. Sales transaction monitoring/checking method

USE - For verifying authenticity of goods purchased or offered for sale over network such as Internet. ADVANTAGE - Since identification code is provided for all products, the validity of purchased product is determined by communicating code of purchased product to authentication server, thus purchasers are enabled to purchase the product with same level of security as in commercial exchanges.

DESCRIPTION OF DRAWINGS - The figure shows system level diagram illustrating the network arrangement and use of such a network arrangement to authenticate goods purchased over the network.

58 Purchaser

62 Server

Original Publication Data by Authority

Australia

Publication No. AU 200078270 A (Update 200170 E)

Publication Date: 20010410

Assignee: ASSURE SYSTEMS INC; US (ASSU-N)

Language: EN

Application: AU 200078270 A 20000906 (Local application)

Priority: US 1999391114 A 19990907

Related Publication: WO 2001018677 A (Based on OPI-patent)

Inventor name & address:

DOLJACK, Frank, A., 750 Montevino Drive, Pleasanton, CA 94566, US, Pleasanton, CA 94566, US NICELY, Mark, C., 1335 Bay Street, 4, San Francisco, CA 94123, US, San Francisco, CA 94123, US DERBYSHIRE, Rodney, 398 Menlo Oaks Drive, Menlo Park, CA 94025, US, Menlo Park, CA 94025, US

DOLJACK, Frank, A., 750 Montevino Drive, Pleasanton, CA 94566, US, US NICELY, Mark, C., 1335 Bay Street, #4, San Francisco, CA 94123, US, US

DERBYSHIRE, Rodney, 398 Menlo Oaks Drive, Menlo Park, CA 94025, US, US

50/T1,TD,TA,AU,1V/32 (Item 32 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0010927935

WPI Acc no: 2001-549924/

Authentication using a cellular phone on the Internet by performing authentication in parallel with accessing of the personal information stored when a user joins the service

Original Titles:

AUTHENTIFIZIERUNGSVERFAHREN UNTER VERWENDUNG EINES ZELLULAREN TELEFONS IM INTERNET

AUTHENTICATION METHOD USING CELLULAR PHONE IN INTERNET

PROCEDE D'AUTHENTIFICATION UTILISANT UN TELEPHONE CELLULAIRE SUR INTERNET

Authentication method using cellular phone in internet

AUTHENTICATION METHOD USING CELLULAR PHONE IN INTERNET

PROCEDE D'AUTHENTIFICATION UTILISANT UN TELEPHONE CELLULAIRE SUR INTERNET

Inventor: EUN T; CHOI HO; KIM GS; LEE GW; LEE JH

Alerting Abstract WO Al

NOVELTY - A line securing high degree encryption and a security device is used between the authentication server (10) of the service company and the Internet site server (20) and a user (30) requests connection. The Internet server transmits authentication information input at the server and requests approval of authentication. The input authentication is compared with the stored information to determine if approval should be granted to the user or not. USE - Authenticating a cellular phone on the Internet.

ADVANTAGE - Preventing danger of hacking and securing safety of electronic payments.

DESCRIPTION OF DRAWINGS - The drawing illustrates the method

- 10 Authentication server
- 20 Internet site server

30 User

Original Publication Data by Authority

Australia

Publication No. AU 200128899 A (Update 200171 E)

Publication Date: 20010731

Assignee: MICROINSPECTION INC; KR (MICR-N)

Language: EN

Application: AU 200128899 A 20010118 (Local application)

Priority: KR 20002771 A 20000118

KR 20005661 A 20000207

Related Publication: WO 2001054438 A (Based on OPI patent)

Current IPC: G06F-1/00(R,N,M,EP,20060101,20051008,A) G06F-1/00(R,N,M,EP,20060101,20051008,C)

G06F-21/00(R,I,M,EP,20060101,20051008,A) G06F-21/00(R,I,M,EP,20060101,20051008,C) H04Q-7/38(R,I,M,EP,20060101,20051008,A) H04Q-7/38(R,I,M,EP,20060101,20051008,C)

Inventor name & address:

EUN, Tak, 204-904 Hyundai Apt., 448 Worlphi-dong, Ansan-shi, Kyunggi-do 425-070, KR, Ansan-shi, Kyunggi-do

425-070, KR CHOI H O,

KIM G S.

LEE G W,

LEEJH.

EUNT.

Eun, Tak, Kyunggi-do, KR, Kyunggi-do, KR

EUN, Tak, 204-904 Hyundai Apt., 448 Worlphi-dong, Ansan-shi, Kyunggi-do 425-070, KR, KR

50/TI,TD,TA,AU,IV/33 (Item 33 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0010926304

WPI Acc no: 2001-548251/

Method for proving paying gateway in internet electronic wallet

Inventor: HAN Y S

Alerting Abstract KR A

NOVELTY - The method for proving a paying gateway in an internet electronic wallet is provided for an internet commercial transaction buyers to identify a paying gateway system easily by inputting personal secret data of internet commercial transaction buyers in a paying gateway system and rendering the paying gateway system to transmit the personal secret data and a characteristics picture seal information to a transaction purchase system. DESCRIPTION - The internet commercial transaction purchase system creates personal secret data and registers the data, a buyer ID and a secret number(ST31). If a purchase demand is transmitted from the internet commercial transaction purchase system, a paying gateway demands the buyer ID and a secret number(ST32). If the inputted buyer ID is pre-registered, pre-registered personal secret data and picture seal information are transmitted to a purchase system(ST33, ST34). If an electronic wallet server is executed and credit information is inputted by the buyer, the paying gateway requests a paying to a card system(ST35). If a paying result is transmitted from the card system, the paying result is transmitted to a selling system (ST36). The selling system decides as to whether a commodity delivery is permitted in accordance with the paying result(ST37).

Original Publication Data by Authority

Inventor name & address: HAN Y S,

50/T1,TD,TA,AU,1V/34 (Item 34 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0010912767

WPI Acc no: 2001-534079/

Banking system and method using smart card

Inventor: CHUNG H W; JUNG H W

Alerting Abstract KR A

NOVELTY - A banking system and a method using a smart card are provided to decode secure information, for example account data, by using a smart card so that it can assure a security of a user information over a public network

DESCRIPTION - The method comprises steps of issuing a banking card storing a user information, an account information, a secret code and a secret key used in coding and host approval(S100), comparing a received user password with the information stored in the issued banking card(S200), generating a service selection and a service format via a client terminal, accessing a banking host, and generating an inter-approval and a coding format(S300), and performing a banking task through a bank computer system and a network by using the generated session(S400). The system comprises the smart card, the client terminal, the banking host, and the bank computer system.

Original Publication Data by Authority

Inventor name & address: JUNG H W, CHUNG H W,

50/T1, TD, TA, AU, IV/35 (Item 35 from file: 350) **Links**

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0010772955

WPI Acc no: 2001-387444/

Secured payment for goods purchased through Internet, involves sending purchaser's access code acquired

from seller to host computer of credit card company which sends delivery information to seller's host computer

Original Titles:

INTERNET TRADE ENHANCING PURCHASER'S SECURITY

SECURITE D'ACHAT ACCRUE POUR TRANSACTIONS SUR L'INTERNET

Inventor: PARK C

Alerting Abstract WO A1

NOVELTY - The purchaser inputs credit card and secret numbers and also access code to Internet card company. Host of credit card company sends purchaser's name and address to seller's computer, for delivery of goods after checking the credit. Seller's computer sends request for payment to credit card company after delivering goods, after which purchaser pays to the credit card company.

DESCRIPTION - Purchaser chooses goods from the seller's homepage. The seller's host sends purchaser's access code to the purchaser.

USE - For secured payment using credit card for goods, services and other information purchased or acquired through Internet.

ADVANTAGE - Seller's host provides purchaser's access code for trade, so that purchaser's credit card secret number is secured. By using the purchaser's identification number, it is possible for the seller's host to write and data for specific purchaser and goods can be searched using temporary identification number.

DESCRIPTION OF DRAWINGS - The figure shows flowchart of payment system using credit card.

Original Publication Data by Authority

Australia

Publication No. AU 200065990 A (Update 200143 E)

Publication Date: 20010305

Assignee: PARK C; KR (PARK-I)

Language: EN (3 pages)

Application: AU 200065990 A 20000808 (Local application)

Priority: KR 199932837 A 19990810

KR 200043903 A 20000728

Related Publication: WO 2001011513 A (Based on OPI patent)

Original IPC: G06F-17/60(A) Current IPC: G06F-17/60(A) Inventor name & address:

PARK C.

PARK, Chul, 701 Hanyang Apt., 396, kukal li, kiheung up, yongin city, Kyungki do 449-900, KR, KR

50/TI,TD,TA,AU,IV/36 (Item 36 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0010555345

WPI Acc no: 2001-158927/

Asset exchange system for facilitating sale of items, includes multi-item optimizer connected to processor which define sales criteria for accepting winning bids from buyers for multiple item listing Original Titles:

SYSTEM AND METHOD FOR PROVIDING AN ELECTRONIC BUSINESS-TO-BUSINESS EXCHANGE FOR BUYERS AND SELLERS

SYSTEME ET PROCEDE ASSURANT DES ECHANGES COMMERCIAUX ELECTRONIQUES ENTRE ACHETEURS ET VENDEURS

Inventor: BOYLE T R; MCCAGG B; SCHILLING P

Alerting Abstract WO A2

NOVELTY - The processor (50) maintains addressable website and controls access to website via Internet by buyer and seller. Multiple sales modules connected to the processor, process sale information of several items as specified by seller. The multi-item optimizer connected to processor, defines sales criteria for accepting winning bids from buyers for multiple item listing.

DESCRIPTION - The processor is configured to query the seller for preferred transaction type comprising first-come-first-served transaction type. The seller provides minimum acceptable bid or standard auction transaction type or highest sealed bid transaction type and item is sold to buyer that enters a bid equal to the minimum acceptable bid. An INDEPENDENT CLAIM is also included for method for facilitating sale of items via asset exchange system.

USE - For providing electronic business-to-business exchange for buyers and sellers via Internet. Also for exchanging purchase orders, sales invoices insurance documents, shipping document payments etc.

ADVANTAGE - Enables user to view and bid for listing available to private sale group, without requiring the user to qualify for private sales group by entering the **account number** or **password**. An **anonymous** remailer **system** is used to alter the buyer's and seller's e-mail addresses, thereby preventing the buyers and sellers from circumventing auction fees by arranging to conduct sale off-site. Regardless of type of transaction selected by seller, same data and same process are employed to determine winning price and winning quantity. Since the buyer's bid increases periodically, it enables buyer to obtain a lower price in event that the seller reduces her minimum acceptable bid price prior to buyer meeting it. The operator of surplus asset exchange **system** can monitor e-mail messages between sellers and buyers by copying the messages to website operator e-mail address. Unless the seller designates a private sales group, the listing is available to all potential buyers.

DESCRIPTION OF DRAWINGS - The figure shows the diagram that illustrates the various components of surplus assets exchange system.

50 Processor

Technology Focus

INDUSTRIAL STANDARDS - The XML/EDI refers to industrial standard for conducting commerce electronically over the Internet.

Original Publication Data by Authority

Australia

Publication No. AU 200044739 A (Update 200116 E)

Publication Date: 20001110

Assignee: TRADEOUT.COM INC; US (TRAD-N)

Language: EN

Application: AU 200044739 A 20000420 (Local application)

Priority: US 1999130607 P 19990422

Related Publication: WO 2000065505 A (Based on OPI patent)

Inventor name & address:

McCAGG, Brin, 119 East 84th Street, #6A, New York, NY 10028, US, US

BOYLE, Thomas, R., 362 Joan Drive, Fairfield, CT 06430, US, US SCHILLING, Peter, 59 Woodleigh Road, Dedham, MA 02026, US, US

50/T1,TD,TA,AU,IV/37 (Item 37 from file: 350) **Links**

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0010461009

WPI Acc no: 2001-060528/

Financial payment system for on-line internet purchases, adjusts electronic account outstanding balance for input electronic account by monetary amount

Original Titles:

FINANCIAL PAYMENT METHOD AND MEDIUM PROCEDE ET SUPPORT DE PAIEMENT FINANCIER

Inventor: BRADEN W; HSIEH P

Alerting Abstract WO Al

NOVELTY - Account number, unique vault code, password and monetary account associated with the particular transaction are received and are compared with that stored in a database which stores electronic account, corresponding to the received account number. If a match exists, the electronic account outstanding balance for input electronic accounts is adjusted by the amount of monetary value.

DESCRIPTION - Each account instrument is associated with a buyer and has an account number, unique vault code and associated password. A database **computer** is linked to a remote gateway **computer**, and stores several electronic accounts associated with several account instruments respectively. Each electronic account consists of data including account number, password and outstanding balance. An INDEPENDENT CLAIM is also included for financial payment method.

USE - For making financial payments via electronic transactions such as on-line internet purchases, for internet based communications and ACH commerce, for consumer accounting or financial planning application. ADVANTAGE - Provides internet merchants with cheaper payment medium alternative to credit cards for acceptance of on-line payments. Provides seller and buyer a method for on-line commerce possessing the key attributes of cash and check while accommodating exigencies of multiple currency and languages. DESCRIPTION OF DRAWINGS - The figure shows the flow chart illustrating purchase transaction.

Original Publication Data by Authority

Inventor name & address:

BRADEN, Wythe, 211 Luika Place, Kailua, HI 96734, US, US HSIEH, Patrick, 7122 Hawaii Kai Drive, #82, Honolulu, HI 96825, US, US

50/TI,TD,TA,AU,IV/38 (Item 38 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0009377926

WPI Acc no: 1999-312506/

Gaming method for conducting game of chance in conjunction with regular sporting events e.g. football Original Titles:

APPARAT UND VERFAHREN ZUM DURCHFUHREN VON GLUCKSSPIELEN

APPARATUS AND METHOD FOR CONDUCTING GAMES OF CHANCE

APPAREIL ET PROCEDE POUR PRATIQUER DES JEUX DE HASARD

Conducting games of chance using predicted sum of scores.

Method and apparatus for conducting games of chance.

APPARATUS AND METHOD FOR CONDUCTING GAMES OF CHANCE

APPAREIL ET PROCEDE POUR PRATIQUER DES JEUX DE HASARD

Inventor: KAIL G

Alerting Abstract WO A2

NOVELTY - A number of sporting events e.g. baseball or football games are identified for play by participants during a given period of time, i.e. on a weekly basis. The winning series of numbers is determined after the identified games have been played to competition, including any extra time, or extra innings etc. The final value of each team's scoring in the identified set is combined to provide a total numerical value.

DESCRIPTION - INDEPENDENT CLAIMS are included for; an apparatus for conducting games of chance n conjunction with a number of sporting events.

USE - Conducting games of chance in which large numbers of participants each pay a fee and select series of numbers in a prescribed range, with the winner being the participants whose numbers correspond to a series of randomly derived numbers.

ADVANTAGE - Scores of one or more alternative like sporting events can be substituted in cases of events not

being completed e.g. due to inclement weather.

DESCRIPTION OF DRAWINGS - The drawing shows a flow chart depicting the steps of the invention.

Original Publication Data by Authority

Australia

Publication No. AU 199919614 A (Update 199937 E)

Publication Date: 19990503

Assignee: SUPRA ENG LTD; IE (SUPR-N)

Language: EN

Application: AU 199919614 A 19981013 (Local application)

Priority: US 1997950243 A 19971014

US 199820128 A 19980206

Related Publication: WO 1999019841 A (Based on OPI patent)

Original IPC: G07C-15/00(A) G06F-17/60(B) Current IPC: G07C-15/00(A) G06F-17/60(B)

Inventor name & address:

KAIL G, KAIL G.

KAIL G.

KAIL, Gianni, Via Moretta, 41, I-10139 Torino, IT, I-10139 Torino, IT

KAIL G.

Kail, Gianni, Turin, IT, IT Kail, Gianni, Turin, IT, IT

KAIL, Gianni, Via Moretta, 41, I-10139 Torino, IT, IT

50/T1,TD,TA,AU,IV/39 (Item 39 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0009076265

WPI Acc no: 1998-506943/

Method for executing secure online transaction between vendor and user computers - send transaction request to vendor computer with user identification data unique to user computer, vendor sends verification request to trust server which authenticates user to authorise transaction when authorisation has passed Original Titles:

VERFAHREN UND SYSTEM ZUR SICHERUNG VON ON-LINE TRANSAKTIONSVERARBEITUNG METHOD AND SYSTEM FOR SECURE ONLINE TRANSACTION PROCESSING

PROCEDE ET SYSTEME DE TRAITEMENT PROTEGE DE TRANSACTION EN DIRECT

Method and system for secure online transaction processing.

METHOD AND SYSTEM FOR SECURE ONLINE TRANSACTION PROCESSING

Inventor: SIXTUS T

Alerting Abstract WO A2

The method allows the user (12) computer to send a transaction request message to the vendor computer (14) via the computer network. The financial transaction request comprises user identification data unique to the user computer. In response to the receipt of the request the vendor computer sends a verification request to a trust server (18) computer interconnected to the computer network.

The verification request has user identification data and data indicating the requested transaction. In response to receiving this request the trust **server** authenticates the user **computer** using the user identification data and communicates with the user **computer** for verification with the user identification data. The trust **server** authorises the transaction when the authentication has passed.

USE - Relates to online electronic commerce and to secure methodology for approving online transaction carried out over Internet.

ADVANTAGE - Authenticates identity and credit of purchaser without transmitting credit card number or other payment mechanism as part of online transaction.

Original Publication Data by Authority

Australia

Publication No. AU 199865494 A (Update 199906 E)

Publication Date: 19980929

Assignee: CHA! TECHNOLOGIES INC (CHAT-N)

Inventor: SIXTUS T Language: EN

Application: AU 199865494 A 19980312 (Local application)

Priority: US 1997816410 A 19970313

Related Publication: WO 1998040809 A (Based on OPI patent)

Original IPC: G06F-19/00(A) Current IPC: G06F-19/00(A) Inventor name & address:

SIXTUS T, SIXTUS T,

SIXTUS, Timothy, 704 Broadway, New York, NY 10003, US, New York, NY 10003, US

SIXTUS T, SIXTUS T.

Sixtus, Timothy, New York, NY, US, US

SIXTUS, TIMOTHY, 704 BROADWAY, NEW YORK, NY 10003, US, US, US

50/TI,TD,TA,AU,IV/40 (Item 40 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0008978309

WPI Acc no: 1998-532243/

Digital payment transaction system operating method e.g. for Internet - having broker generating and storing secret number and generating chain of hash values by successive operations of hash functions, using secret number as starting value with broker issuing too user, digitally encoded value

Original Titles:

TRANSAKTIONSSYSTEM
TRANSACTION SYSTEM
SYSTEME TRANSACTIONNEL
Electronic coin stick with potential for future added value.

TRANSACTION SYSTEM Inventor: BRISCOE R J

Alerting Abstract WO Al

The method involves, at a first party, ("the broker") generating a secret number. The secret number is stored at the first party. A hash chain of values which are derived from the secret number by successive operations of a hash function are generated at the party. A digitally encoded value is communicated to a second party ("the user") from the chain of hash values. At the second party a second hash chain of values are generated which are derived from the value communicated by the first party.

Digitally encoded values are communicated from the second hash chain to a third party ("the vendor") in payment. A value is subsequently communicated to the second party from the first party in the hash chain which precedes the value originally communicated.

ADVANTAGE - Provides method of using coin stick between three parties. Increases flexibility in operation of transaction system, for use in on-line trading with multiplicity of vendors.

Original Publication Data by Authority

Australia

Publication No. AU 199867401 A (Update 199909 E)

Publication Date: 19981020

Assignce: BRITISH TELECOM PLC (BRTE)

Inventor: BRISCOE R J

Language: EN

Application: AU 199867401 A 19980323 (Local application)

Priority: EP 1997302098 A 19970326

Related Publication: WO 1998043211 A (Based on OPI patent)

Original IPC: G07F-7/10(A) Current IPC: G07F-7/10(A) Inventor name & address:

BRISCOE R J,

BRISCOE, Robert, John, Home Farm, Parham, Woodbridge, Suffolk 1P13 9NW, GB, Woodbridge, Suffolk 1P13

9NW. GB

Briscoe, Robert J, Suffolk, GB, GB

BRISCOE, ROBERT, JOHN, HOME FARM, PARHAM, WOODBRIDGE SUFFOLK 1P13 9NW, GB, GB, GB

50/TI,TD,TA,AU,IV/41 (Item 41 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0008918697

WPI Acc no: 1998-469511/

Satellite receiver method for on-line banking using IC card - involves adapting satellite receiver to act as banking terminal for modem connection to bank and performing banking services

Original Titles:

Empfanger mit der Funktion eines Elektronischen Geldautomaten und Verfahren zum ausfuhren dieser Funktion Empfaenger mit der Funktion eines Elektronischen Geldautomaten und Verfahren zum ausfuehren dieser Funktion Receiver having electronic money terminal function and method for performing this function Recepteur ayant la fonction de terminal de monnaie electronique et methode pour executer cette fonction Empfanger mit der Funktion eines Elektronischen Geldautomaten und Verfahren zum ausfuhren dieser Funktion Receiver having electronic money terminal function and method for performing this function Recepteur ayant la fonction de terminal de monnaie electronique et methode pour executer cette fonction RECEIVER WITH BUILT-IN ELECTRONIC MONEY TERMINAL FUNCTION AND ITS IMPLEMENTING METHOD

Method and apparatus for performing an electronic money terminal function using a smart card.

Inventor: PARK J; PARK J H

Alerting Abstract EP A2

The method using a TV tuner and electronics to provide a user with free, subscription or pay by view services. It contains an IC card reader and modem to handle subscription and pay per view controls. The receiver also has menu functions providing access to banking services. When the banking functions are selected, the receiver contacts a host computer by modem.

It transmits the type of service required and PIN. The host then asks for the user secret code which can be entered and sent. A menu is then used to allow the user to operate various banking functions. This includes recharging the IC card or other transfer functions.

ADVANTAGE - Allows the user to recharge an IC card from a convenient location rather than visiting a bank

machine.

Original Publication Data by Authority

Inventor name & address:

Park, Ji-ha, 101-605, Dujin Apt., Youngduck-ri, Kiheung-eub, Yongin-city, Kyungki-do, KR, KR, KR
Park, Ju-ha, 101-605, Dujin Apt., Youngduck-ri, Kiheung-eub, Yongin-city, Kyungki-do, KR, Yongin-city,
Kyungki-do, KR
PARK JI-HA,
PARK J,
PARK J H,
Park, Ju-ha, Yongin, KR, KR

50/TI,TD,TA,AU,IV/42 (Item 42 from file: 350) **Links**

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0007759262

WPI Acc no: 1996-384055/

Electronics fund transfer system e.g automated teller machine - has input device which enables user to select custom transaction from customised menu for execution and control device executes selected transaction Original Titles:

SYSTEM ZUM TRANSFERIEREN VON ELEKTRONISCHEN GELDMITTELN ELECTRONIC FUND TRANSFER SYSTEM TRANSFERTS ELECTRONIQUES DE FONDS Electronic fund transfer system. ELECTRONIC FUND TRANSFER SYSTEM

Inventor: GATTO J G

Alerting Abstract US A

The system includes a user identification cards unique to each user and having information stored which includes transaction information corresponding to custom transactions pre-defined by the user of the identification card. A user accessible transaction terminal which includes card reader device for reading information stored on the user identification card.

A display device displays a user customised menu comprising one or more of the custom transactions based on information read from the user's identification card. An input device enables the user to select a custom transaction from the customised menu for execution. A control device executes a selected transaction.

ADVANTAGE - Provides customised menu for individual user. Enables user-defined transaction to be completed with reduced number of inputs from user.

Original Publication Data by Authority

Australia

Publication No. AU 708287 B (Update 199941 E)

Publication Date: 19990729

Assignee: GATTO J G; US (GATT-I)

Language: EN

Application: AU 199655448 A 19960412 (Local application)

Priority: US 1995421486 A 19950413

Related Publication: AU 9655448 A (Previously issued patent)

WO 1996032687 A (Based on OPI patent) Original IPC: G06F-17/60(A) G06F-15/00(B) Current IPC: G06F-17/60(A) G06F-15/00(B)

Publication No. AU 199655448 A (Update 199708 E)

Publication Date: 19961030 Assignee: GATTO J G (GATT-I)

Inventor: GATTO J G

Language: EN

Application: AU 199655448 A 19960412 (Local application)

Priority: US 1995421486 A 19950413

Related Publication: WO 1996032687 A (Based on OPI patent)

Original IPC: G06F-17/60(A) G06F-15/00(B) Current IPC: G06F-17/60(A) G06F-15/00(B)

Inventor name & address:

GATTO J G,

Gatto, James G., 1101 Mountain Hope Court, Great falls, VA 22066, US, US, US

Gatto, James G.,

GATTO, JAMES, G., US, US, US

50/TI,TD,TA,AU,IV/43 (Item 43 from file: 347) Links JAPIO (c) 2007 JPO & JAPIO. All rights reserved.

NAME SORTING CONTROL METHOD

Inventor: SATO YOSHINORI MORITA TOYOHISA MAKI HIDEYUKI FUKUMOTO YASUSHI 50/TI,TD,TA,AU,IV/44 (Item 44 from file: 347) Links

JAPIO

(c) 2007 JPO & JAPIO. All rights reserved.

INFORMATION PROCESSOR FOR SUPPORTING INTEGRATED MANAGEMENT OF ACCOUNT SERVICE INFORMATION, INTEGRATED MANAGEMENT METHOD FOR ACCOUNT SERVICE INFORMATION, PROGRAM, AND RECORDING MEDIUM

Inventor: HIRAMATSU KENTAI

>>>W: Some display codes not found in file 347: TD TA IV

50/TI,TD,TA,AU,IV/45 (Item 45 from file: 347) Links

JAPIO

(c) 2007 JPO & JAPIO. All rights reserved.

ELECTRONIC BUSINESS TRANSACTIONS SERVER, ELECTRONIC BUSINESS TRANSACTIONS SYSTEM, ELECTRONIC BUSINESS TRANSACTIONS METHOD AND PROGRAM

Inventor: SAKAMOTO HIROAKI

50/T1,TD,TA,AU,IV/46 (Item·46 from file: 347) Links

JAPIO

(c) 2007 JPO & JAPIO. All rights reserved.

SYSTEM FOR TRACKING ACTIVITY OF USER IN ELECTRONIC COMMERCE SYSTEM

Inventor: SAM JOSEPH

3/5/1 (Item 1 from file: 350) Links

Derwent WPIX

(c) 2007 The Thomson Corporation. All rights reserved.

0011000652 Drawing available WPI Acc no: 2001-625823/200172 XRPX Acc No: N2001-466513

Enabling anonymous credit transactions for the purchase of good and services from merchants over e.g. the

internet

Patent Assignee: E-SCORING INC (ESCO-N)
Inventor: BRODY R M; KENNEDY R S

Patent Family (4 patents, 93 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
WO 2001065502	A2	20010907	WO 2001US6445	A	20010228	200172	В
US 20010029485	A1	20011011	US 2000186166	P	20000229	200172	Е
			US 2001796719	Α	20010228		
AU 200139945	A	20010912	AU 200139945	A	20010228	200204	E
AU 2001239945	A8	20051006	AU 2001239945	Α	20010228	200612	Е

Priority Applications (no., kind, date): US 2001796719 A 20010228; US 2000186166 P 20000229

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
WO 2001065502	A2	EN	28	3		
National Designated States,Original	CZ DE DK DM I KE KG KP KR K MX MZ NO NZ UG US UZ VN Y	OZ EI IZ LC PL P 'U Z <i>I</i>	E ES C LK Γ RC A ZV	FI GE LR LS RU S V	BB BG BR BY BZ CA C GD GE GH GM HR HI S LT LU LV MA MD M D SE SG SI SK SL TJ T	J ID IL IN IS JP G MK MN MW M TR TT TZ UA
Regional Designated States,Original	AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW					
US 20010029485	A1	EN			Related to Provisional	US 2000186166
AU 200139945	A	EN			Based on OPI patent	WO 2001065502
AU 2001239945	A8	EN			Based on OPI patent	WO 2001065502

Alerting Abstract WO A2

NOVELTY - Blocks of consumer credit card numbers are used to create dynamic mappings of the card numbers to account numbers or even other card numbers, e.g. pseudo-random credit card numbers. Because pseudo-random attributes are transmitted to the merchant; the transaction between the consumer and merchant will be anonymous. USE - Enables consumers to purchase goods and services from merchants, using credit cards.

ADVANTAGE - Consumers can maintain the confidentiality of their credit card numbers and identity without

disclosure to the merchants.

DESCRIPTION OF DRAWINGS - The drawing shows a schematic diagram of the system employing the method.

Title Terms /Index Terms/Additional Words: ENABLE; CREDIT; TRANSACTION; PURCHASE; SERVICE; MERCHANT

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-017/60; G07F-007/10			Main		"Version 7"
G07F-019/00; H04K-001/00			Secondary		"Version 7"

US Classification, Issued: 705039000, 705075000

File Segment: EPI;

DWPI Class: T01; T05

Manual Codes (EPI/S-X): T01-E04; T01-H07C5E; T01-J05A1; T05-H02C3; T05-L02

```
Description
Set
        Items
                S COMPUTER? ? OR CPU? ? OR CENTRAL() PROCESSING OR PROCESSOR? ? OR SERVER?
S1
      1663274
? OR MINICOMPUTER? ? OR MICROCOMPUTER? ? OR PC OR LAPTOP? ? OR HANDHELD? ? OR NOTEBOOK? ?
OR COMPUTING OR MAINFRAME? ? OR MAIN()(FRAME OR FRAMES) OR SYSTEM? ? OR SELF()SERVIC? OR
ATM OR ATMS OR ((AUTOMATED OR AUTOMATIC)()(TELLER OR TRANSACTION OR SERVICE) OR CASH OR
MONEY OR BANK) (W) (MACHINE? OR TERMINAL? ?) OR ELECTRONIC() TELLER? ?
                S VIRTUAL OR ONLINE OR ON()LINE OR INTERNET OR NET OR WEB OR WWW OR CYBER
      702319
OR ELECTRONIC OR WEBSITE? OR WEBPAGE? OR WEB()(SITE? OR SERVER? ?)
                S ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNSPECIF? OR
      206516
UNKNOWN OR "NO" (2N) (PERSONAL OR USER)
                S DATA OR DEMOGRAPHIC? ? OR INFORMATION OR NUMBER? ? OR IDENTIFICATION OR
      1630041
NAME? ? OR ID
                S PASSWORD OR PIN OR PERSONAL()(IDENTIFICATION OR ID)()NUMBER OR CODE OR
       578273
KEY OR (PASS OR SECRET) () (WORD? ? OR PHRASE? ? OR NUMBER? ?) OR PASSPHRASE OR PASSNUMBER
OR (SECURITY OR ACCESS)()(CODE? ? OR KEY? ?) OR USER()(ID OR IDENTIFICATION OR NAME)
                S LOGON OR LOGIN OR (LOG OR LOGG? OR SIGN OR SIGNING OR SIGNED) () (IN OR
       193584
ON) OR AUTHENTICAT? OR (UNIQUE OR UNCOMMON OR DISTINGUISHING OR
DISTINCTIVE) (10N) (INFORMATION OR DATA OR STATISTIC? ? OR NUMBER? ?)
                S PATRON? ? OR CUSTOMER? ? OR CLIENT? ? OR USER? ? OR SUBSCRIBER? ? OR
ENROLEE? ? OR PARTICIPANT? ? OR PARTICIPAT?R? ? OR PERSON? ? OR DRIVER? ? OR OPERATOR? ?
(5N) GENERAT ??? OR ACCOMPLISH? OR BRING() ABOUT OR CREATE? OR FORM? ? OR INITIAT?
                S TRANSACTION? ? OR ACCOUNT? ? OR INTERACTION? ? OR ACTION? ? OR
       857472
PURCHAS??? OR DEAL? ?
                S S3(5N)S4
        29710
S9
                S S3(5N)S5
        18038
S10
                S S3(5N)S6
         3359
S11
         6805
               S S9(5N)(S5 OR S6)
S12
         2160
               S S12(5N)S7
S13
                S S13(10N)(S1 OR S2)
          778
S14
                S S14 (10N) S8
          119
S15
           63
                S (S13(5N)S1)(5N)S8
S16
           10 .
                S S16 AND IC=G06F-017/60
S17
 ; show files
```

[File 348] EUROPEAN PATENTS 1978-2007/ 200705

(c) 2007 European Patent Office. All rights reserved.

|File 349| PCT FULLTEXT 1979-2007/UB=20070201UT=20070125

(c) 2007 WIPO/Thomson. All rights reserved.

^{*}File 348. For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.

^{*}File 349: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.

17/3K/1 (Item 1 from file: 348) Links

EUROPEAN PATENTS

(c) 2007 European Patent Office. All rights reserved.

01497543

NET ORDER SYSTEM

NETZ-BESTELLSYSTEM

SYSTEME DE COMMANDE SUR INTERNET

Patent Assignee:

• FUJITSU TEN LIMITED; (300132)

1-2-28 Gosho-dori, Hyogo-ku; Kobe-shi, Hyogo 652-8510; (JP) (Applicant designated States: all)

Inventor:

• MISHIMA, Masayuki, C/O FUJITSU TEN LTD

2-28, Gosho-dori 1-chome, Hyogo-ku; Kobe-shi, Hyogo 652-8510; (JP)

Legal Representative:

• Skone James, Robert Edmund (50281)

GILL JENNINGS & EVERY Broadgate House 7 Eldon Street; London EC2M 7LH; (GB)

	Country	Number	Kind	Date	
Patent	EP	1367517	Al	20031203	(Basic)
	WO	2002073486		20020919	
Application	EP	2002702839		20020308	
11	WO	2002JP2195		20020308	
Priorities	JР	200165099		20010308	

Designated States:

AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR;

Extended Designated States:

AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-017/60; G06F-017/60Abstract Word Count: 120

NOTE: 03

NOTE: Figure number on first page: 03

		W 7 9 1	7004
Tuno	Pub. Date	Kind	Text
Type	I ub. Date	Izilia	
J			

Publication: English Procedural: English Application: Japanese

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200349	221
SPEC A	(English)	200349	3057
Total Word Count (Document A) 3278			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 3278			

Specification: ...transaction. In this case, unlike the credit-card transactions through the Internet, transmission of a **secret number** is not required. This is effective for protecting individual information, which has good influence on. **users**' psychology and promotes the expansion of the Internet sales.

In any cases, the product itself is directly delivered to the **user** 14 in order to take advantages of the direct-selling **system** through the Internet. However, it is possible to make the delivery to the sales outlet where the **user purchased** the product or a specific convenience store, other than using the home delivery service to the **user**'s house.

If a credit-card is used, a check is performed by connecting to... ... case of the second time or later, confirmation can be performed by the past order data (ID code and secret code is given at the time of first order)).

As mentioned above, according to the present...

17/3K/2 (Item 2 from file: 348) **Links**

EUROPEAN PATENTS

(c) 2007 European Patent Office. All rights reserved.

01492506

PAYMENT STATEMENT ISSUING SYSTEM AND CHARGE PAYING SYSTEM

BEZAHLUNGSAUFFUHRUNGSAUSGABESYSTEM UND GEBUHRENBEZAHLUNGSSYSTEM SYSTEME D'EDITION D'ETATS DE PAIEMENT ET SYSTEME DE PAIEMENT DE DEBITS

Patent Assignee:

- Kunugi, Takanobu; (2956780) 558-18, Shimoyasumatu; Tokorozawa-shi, Saitama 359-0024; (JP) (Applicant designated States: all)
- Kunugi, Yurako; (2956790) 558-18, Shimoyasumatu; Tokorozawa-shi, Saitama 359-0024; (JP) (Applicant designated States: all)

Inventor:

- KUNUGI, Takanobu 558-18 Shimoyasumatu Tokorozawa-shi; Saitama 359-0024; (JP)
- KUNUGI, Yurako

558-18 Shimoyasumatu Tokorozawa-shi; Saitama 359-0024; (JP)

Legal Representative:

• Klunker . Schmitt-Nilson . Hirsch (101001)

Winzererstrasse 106; 80797 Munchen; (DE)

	Country	Number	Kind	Date	
Patent	EP	1345139	Al	20030917	(Basic)
-	WO	2002050735		20020627	, , , , , , , , , , , , , , , , , , , ,
Application	EP	2001271119		20011217	
	WO	2001JP11041		20011217	
Priorities	JР	2000383294		20001218	
	JP	2000398679		20001227	
	JP	2001377410		20011211	

Designated States:

DE; FR; GB; IT;

Extended Designated States:

AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-017/60; G06F-017/60Abstract Word Count: 184

NOTE: 7

NOTE: Figure number on first page: 7

Type	Pub. Date	Kind	Text
D 11' (' E 1' 1			

Publication: English
Procedural: English
Application: Japanese

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200338	1292
SPEC A	(English)	200338	9670
Total Word Count (Document A) 10962			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 10962			

Specification: ...a user's secret identification code in a financial institution where the user has an account; means for sending the entered secret identification code, amount information, and user's account information to a computer system of the financial institution, so as to check whether a payment through account transfer...

Claims: ...a user's secret identification code in a financial institution where the user has an account;

means for sending the entered secret identification code, amount information, and user's account information to a computer system of the

17/3K/3 (Item 1 from file: 349) **Links**

PCT FULLTEXT

(c) 2007 WIPO/Thomson. All rights reserved.

01019913

PAYMENT APPARATUS AND METHOD USING TRANSFER CARD

APPAREIL ET PROCEDE DE PAIEMENT AU MOYEN D'UNE CARTE DE TRANSFERT

Patent Applicant/Patent Assignee:

• DIGITAL SERVICE CO LTD; #202, K.J. Building, 6-39 yangjae-dong, seocho-gu, 137-886 Seoul KR; KR(Residence); KR(Nationality) (For all designated states except: US)

• KIM Young-Jin; #302, shalom house, 699-4, yeoksam-dong, Gangnam-gu, 135-917 Seoul

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

Patent Applicant/Inventor:

• KIM Young-Jin

#302, shalom house, 699-4, yeoksam-dong, Gangnam-gu, 135-917 Seoul; KR; KR(Residence); KR(Nationality); (Designated only for: US)

Legal Representative:

• JOO Won-Tae(agent)

Synergy International Patent and Law Office, 2F., T.S.K. Bldg., 834-20, Yeoksam-dong, Kangnam-Gu, 135-080 Seoul; KR:

	Country	Number	Kind	Date
Patent	· WO	200348882	A2-A3	20030612
Application -	WO	2002KR2257		20021130
Priorities	KR	200175638		20011201

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;

FI; FR; GB; GR; IE; IT; LU; MC; NL; PT;

SE; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;

ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;

UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	Level
G06F-017/60	Main

Publication Language: English Filing Language: English Fulltext word count: 5281

Detailed Description:

...to access an electronic commerce site and purchase the commodity by using his transfer card **number** and **secret number** through his personal communication means 300 without using the transfer card 100 as described above... ...the transfer card user to purchase the commodity by the entering of the transfer card **number** and the **secret number**.

Accordingly, the electronic commerce site server 600 receives the data outputted from the personal communication means 300, provides information on the purchasing the commodity to the transfer card **user**, and outputs commodity purchase information. The financial settlement system 700 receives the commodity purchase information... site server 600 to process credit conditions according to the use of the transfer card **number** and the **secret number**, **authenticates** the credit conditions, and additionally outputs a control signal corresponding to the authenticated result.

At...

Claims:

...financial settlement system, whether the transfer card user purchases a commodity using a transfer card number and a secret number 1 5 through a personal communication means, if the transfer card user does not purchase...transfer card at step a);g) ending the alternative payment method, if the transfer card user does not purchase the commodity using the transfer card number and the secret number through the personal communication means, and receiving the alternative the 2 0 payment limit informationwith the alternative payment limit information by the financial settlement system, if the transfer card user purchases the commodity using the 2 5 transfer card number and the secret number through the personal communicationmeans;h) performing second authentication for credit conditions of the transfer...

17/3K/4 (Item 2 from file: 349) **Links**

PCT FULLTEXT

(c) 2007 WIPO/Thomson. All rights reserved.

01019912

ALTERNATIVE PAYMENT APPARATUS AND METHOD USING BARCODE STORED IN MOBILE COMMUNICATION TERMINAL

APPAREIL ET PROCEDE DE PAIEMENT ALTERNATIF AU MOYEN D'UN CODE À BARRES STOCKE

DANS UN TERMINAL DE COMMUNICATION MOBILE

Patent Applicant/Patent Assignee:

• DIGITAL SERVICE CO LTD; #202, K.J. Building, 6-39 yangjae-dong, seocho-gu, 137-886 SEOUL

KR; KR(Residence); KR(Nationality) (For all designated states except: US)

• KIM Young-Jin; #302, shalom house, 699-4, yeoksam-dong, Gangnam-gu, 135-917 SEOUL

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

Patent Applicant/Inventor:

• KIM Young-Jin

#302, shalom house, 699-4, yeoksam-dong, Gangnam-gu, 135-917 SEOUL; KR; KR(Residence); KR(Nationality); (Designated only for: US)

Legal Representative:

• JOO Won-Tae(agent)

Synergy International Patent and Law Office, 2F., T.S.K. Bldg., 834-20, Yeoksam-dong, Kangnam-Gu, 135-080 Seoul; KR;

	Country	Number	Kind	Date
Patent	WO	200348881	A2-A3	20030612
Application	WO	2002KR2256		20021130
Priorities	KR	1020010075637		20011201

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;

FI: FR: GB: GR; IE: IT; LU; MC; NL; PT;

SE; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;

ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;

UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	Level
G06F-017/60	 Main

Publication Language: English

Filing Language: English Fulltext word count: 5779

Detailed Description:

...access an electronic commerce site 2 0 and purchase a commodity by using a barcode **number** and a **secret number** through his personal communication means 300 without using the barcode stored in the mobile communication... ...so as to allow the Internet user to purchase a commodity by entering a barcode **number** and a **secret number**.

2 5 Accordingly, the electronic commerce site server 600 receives the data outputted from the to the purchase of the commodity by the Internet user, and outputs commodity purchasing information related to payment. The financial settlement system 700 receives the.....commerce site server 600 to process credit conditions according to the use of the barcode number and the secret number, authenticates the credit conditions, and additionally outputs a control signal corresponding to the authenticated result.

Át...

Claims:

...comprising the steps of 5 g) determining, by the financial settlement system, whether the Internet user purchases a commodity using a barcode number and a secret number through personal communication means, if the Internet user does not purchase a commodity using the 0 h) ending the alternative payment method, if the Internet user does not purchase a commodity using a barcode number and a secret number through the personal communication means, and receiving alternative the payment limit information outputted from the... ...information with secondcommodity purchasing price information by the financial settlement system, if the Internet user purchases a commodity using the barcode number and the secret number through the personal communication means;i) performing

17/3K/5 (Item 3 from file: 349) **Links**

PCT-FULLTEXT

(c) 2007 WIPO/Thomson. All rights reserved.

01013784

PAYMENT APPARATUS AND METHOD USING BARCODE STORED IN MOBILE COMMUNICATION TERMINAL

DISPOSITIF ET PROCEDE POUR LE PAIEMENT SELON UN CODE BARRES ENREGISTRE DANS UN TERMINAL DE COMMUNICATIONS MOBILES

Patent Applicant/Patent Assignee:

• DIGITAL SERVICE CO LTD; #202, K.J. Building, 6-39 yangjae-dong, seocho-gu, 137-886 SEOUL KR; KR(Residence); KR(Nationality) (For all designated states except: US)

KIM Young-Jin; #302, shalom house, 699-4, Yeoksam-dong, Gangnam-gu, 135-917 SEOUL

KR: KR(Residence); KR(Nationality)

(Designated only for: US)

Patent Applicant/Inventor:

KIM Young-Jin

#302, shalom house, 699-4, Yeoksam-dong, Gangnam-gu, 135-917 SEOUL; KR; KR(Residence); KR(Nationality); (Designated only for: US)

Legal Representative:

JOO Won-Tae(agent)

Synergy International Patent and Law Office, 2F., T.S.K. Bldg., 834-20, Yeoksam-dong, Kangnam-Gu, 135-080 Seoul: KR:

	Country	Number	Kind	Date
Patent	WO	200342776	A2-A3	20030522
Application	WO	2002KR2099		20021111
Priorities	KR	200170216		20011112

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;

FI; FR; GB; GR; IE; IT; LU; MC; NL; PT;

SE; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;

ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;

UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

	PC	Level
G06F-017/60	•	Main

Publication Language: English

Filing Language:

English

Fulltext word count: 5881

Detailed Description:

...outputted from the financial settlement system 1000.

5 Meanwhile, if the Internet user desires to purchase a commodity using @L barcode number and a secret number

without using the barcode stored in the mobile communication terminal 100, the Internet user accesses an electronic cominerce site using a mouse (not shown) connected to the personal communication means 800 (for example, desktop computer, notebook computer, 0 etc.) used by the Internet user, selects a desired commodity, and enters a barcode number, a secret number and data required to purchase a commodity using a keyboard (not shown).

The electronic commerce site server 900 then receives... database server 500. The member database server 500 stores commodity purchasing information of the commodity **purchased** using the barcode **number** and the **secret number** of the Internet **user**.

Further, the member database **server** 500 checks a commodity purchasing type of the Internet **user**. That is, the member database **server** 500 outputs a control signal corresponding to the commodity purchasing type according to 1 0 whether the Internet **user** uses the barcode of the mobile communication terminal 100 or whether the Internet **user** uses the barcode **number** and the **secret number** through the personal communication terminal 800.

At this time, if the Internet user uses the ...

17/3K/6 (Item 4 from file: 349) <u>Links</u> PCT FULLTEXT

(c) 2007 WIPO/Thomson. All rights reserved.

00963611

EXTENDED WEB ENABLED MULTI-FEATURED BUSINESS TO BUSINESS COMPUTER SYSTEM FOR RENTAL VEHICLE SERVICES

SYSTEME INFORMATIQUE INTERENTREPRISES A ELEMENTS MULTIPLES A ACCES INTERNET POUR SERVICES DE LOCATION DE VEHICULES

Patent Applicant/Patent Assignee:

• THE CRAWFORD GROUP INC; 600 Corporate Park Drive, St. Louis, MO 63105 US; US(Residence); US(Nationality)

(For all designated states except: US)

• WEINSTOCK Timothy Robert; 1845 Highcrest Drive, St. Charles, MO 63303

US; US(Residence); US(Nationality)

(Designated only for: US)

• DE VALLANCE Kimberly Ann; 2037 Silent Spring Drive, Maryland Heights, MO 63043

US; US(Residence); US(Nationality)

(Designated only for: US)

• HASELHORST Randall Allan; 1016 Scenic Oats Court, Imperial, MO 63052

US; US(Residence); US(Nationality)

(Designated only for: US)

• KENNEDY Craig Stephen; 9129 Meadowglen Lane, St. Louis, MO 63126

US; US(Residence); US(Nationality)

(Designated only for: US)

• SMITH David Gary; 10 Venice Place Court, Wildwood, MO 63040

US; US(Residence); US(Nationality)

(Designated only for: US)

• TINGLE William T; 17368 Hilltop Ridge Drive, Eureka, MO 63025

US; US(Residence); US(Nationality)

(Designated only for: US)

• KLOPFENSTEIN Anita K; 433 Schwarz Road, O'Fallon, JL 62269

US; US(Residence); US(Nationality)

(Designated only for: US)

Patent Applicant/Inventor:

• WEINSTOCK Timothy Robert

1845 Higherest Drive, St. Charles, MO 63303; US; US(Residence); US(Nationality); (Designated only for: US)

DE VALLANCE Kimberly Ann

2037 Silent Spring Drive, Maryland Heights, MO 63043; US; US(Residence); US(Nationality); (Designated only for: US)

• HASELHORST Randall Allan

1016 Scenic Oats Court, Imperial, MO 63052; US; US(Residence); US(Nationality); (Designated only for: US)

KENNEDY Craig Stephen

9129 Meadowglen Lane, St. Louis, MO 63126; US; US(Residence); US(Nationality); (Designated only for: US)

• SMITH David Gary

10 Venice Place Court, Wildwood, MO 63040; US; US(Residence); US(Nationality); (Designated only for: US)

• TINGLE William T

17368 Hilltop Ridge Drive, Eureka, MO 63025; US; US(Residence); US(Nationality); (Designated only for: US)

• KLOPFENSTEIN Anita K

433 Schwarz Road, O'Fallon, IL 62269; US; US(Residence); US(Nationality); (Designated only for: US)

Legal Representative:

• HAFERKAMP Richard E(et al)(agent)

Howell & Haferkamp, L.C., Suite 1400, 7733 Forsyth Blvd., St. Louis, MO 63105-1817; US;

,	Country	Number	Kind	Date
Patent	WO	200297700	A2	20021205
Application	WO	2001US51431		20011019
Priorities	US	2000694050		20001020

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;

GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;

ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;

UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

	IPC	Level
G06F-017/60		Main

Publication Language: English Filing Language: English Fulltext word count: 237932

Detailed Description:

...found that even despite the built-in error checking and 'correction facilities provided to the users of the system, a

repetitive pattern of mistakes ...since the ECOOEXV1 program processing does not update Bill-To Customer information in the rental system database files. (See

@Improvement Opportunities number 3 below.)

;.@-IF processing :an Extension, move an 'aEff to the **Action Code** in the AM055V1 external data structure. When a termination date has been sent, update the...

17/3K/7 (Item 5 from file: 349) **Links**

PCT FULLTEXT

(c) 2007 WIPO/Thomson. All rights reserved.

00933152

EXTENDED WEB ENABLED MULTI-FEATURED BUSINESS TO BUSINESS COMPUTER SYSTEM FOR RENTAL VEHICLE SERVICES

SYSTEME INFORMATIQUE ETENDU ENTRE ENTREPRISES, A FONCTIONS MULTIPLES, FONCTIONNANT SUR LE WEB, POUR DES SERVICES DE LOCATION DE VEHICULES

Patent Applicant/Patent Assignee:

• THE CRAWFORD GROUP INC; 600 Corporate Park Drive, St. Louis, MO 63105 US: US(Residence): US(Nationality)

(For all designated states except: US)

• WEINSTOCK Timothy Robert; 1845 Highcrest Drive, St. Charles, MO 63303 US; US(Residence); US(Nationality)

(Designated only for: US)

• DE VALLANCE Kimberly Amm; 2037 Silent Spring Drive, Maryland Heights, MO 63043

US; US(Residence); US(Nationality)

(Designated only for: US)

• HASELHORST Randall Allan; 1016 Scenic Oats Court, Imperial, MO 63052

US: US(Residence); US(Nationality)

(Designated only for: US)

• KENNEDY Craig Stephen; 9129 Meadowglen Lane, St. Louis, MO 63126

US; US(Residence); US(Nationality)

(Designated only for: US)

• SMITH David Gary; 10 Venice Place Court, Wildwood, MO 63040

US; US(Residence); US(Nationality)

(Designated only for: US)

• TINGLE William T; 17368 Hilltop Ridge Drive, Eureka, MO 63025

US; US(Residence); US(Nationality)

(Designated only for: US)

• KLOPFENSTEIN Anita K; 433 Schwarz Road, O'Fallon, IL 62269

US; US(Residence); US(Nationality)

(Designated only for: US)

Patent Applicant/Inventor:

WEINSTOCK Timothy Robert

1845 Highcrest Drive, St. Charles, MO 63303; US; US(Residence); US(Nationality); (Designated only for: US)

• DE VALLANCE Kimberly Amm

2037 Silent Spring Drive, Maryland Heights, MO 63043; US; US(Residence); US(Nationality); (Designated only for: US)

• HASELHORST Randall Allan

1016 Scenic Oats Court, Imperial, MO 63052; US; US(Residence); US(Nationality); (Designated only for: US)

• KENNEDY Craig Stephen

9129 Meadowglen Lane, St. Louis, MO 63126; US; US(Residence); US(Nationality); (Designated only for: US)

• SMITH David Gary

10 Venice Place Court, Wildwood, MO 63040; US; US(Residence); US(Nationality); (Designated only for: US)

TINGLE William T

17368 Hilltop Ridge Drive, Eureka, MO 63025; US; US(Residence); US(Nationality); (Designated only for: US)

KLOPFENSTEIN Anita K

433 Schwarz Road, O'Fallon, IL 62269; US; US(Residence); US(Nationality); (Designated only for: US)

Legal Representative:

• HAFERKAMP Richard E(et al)(agent)

HOWELL & HAFERKAMP, L.C., Suite 1400, 7733 Forsyth Blvd., St. Louis, MO 63105-1817; US;

	Country	Number	Kind	Date
Patent	WO	200267175	A2_	20020829
Application	WO	2001US51437		20011019
Priorities	US	2000694050		20001020

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;

GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;

ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;

UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC		Level
G06F-017/60	Main	· .

Publication Language: English
Filing Language: English
Fulltext word count: 243912

Detailed Description:

...the implementation of additional functionalities which are engendered by the browser/GUI interface. As the **system** is continuously used,, and feedback is continuously monitored and analyzed, additional features that add value through providing management **information** as well as by speeding **transaction** activity over the **system** may be implemented. For example, several of these features include the ability of a user...Read file EDPREF1 to retrieve the direct billing trading partner's RTs, NETWORK and SCRIPT **information**.

- If **no** record is found a return **code** of 1 indicating nothing can be Deessed.

Dcess

erarchical numeric ID: 1 1 2

ded...file.

-IF any new approved surcharges were generated, then read this file for s rental transaction to generate a new automatic pseudo-rental Authorization mge (AT) transaction set for approved surcharges to be routed to a distributed ital application system host platform...

17/3K/8 (Item 6 from file: 349) **Links**

PCT FULLTEXT

(c) 2007 WIPO/Thomson. All rights reserved.

00874876

ELECTRONIC PAYMENT SYSTEM ON INTERNET AND METHOD THE SAME

SYSTEME DE PAIEMENT ELECTRONIQUE SUR L'INTERNET ET PROCEDE ASSOCIE

Patent Applicant/Inventor:

KIM Kwang-Chul

110-501 LG Apt., 1398 Jwa-dong, Haeundae-gu, Busan 612-768; KR; KR(Residence); KR(Nationality);

Legal Representative:

• JUNG Hyun-Young(agent)

3rd Floor Namsung B/D, 1474-12 Silim 11-dong, Kwanak-gu, Seoul 151-021; KR;

	Country	Number	Kind	Date
Patent	WO	200208988	Al	20020131
Application	WO	2001KR902		20010529
Priorities	KR	200039210		20000710

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;

GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GW; ML;

MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;

UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	Level
G06F-017/60	Main

Publication Language: English Filing Language: Korean

Fulltext word count: 5687

Detailed Description:

...on the financial company server 16. Accordingly, if the client applies for issuance of the client account and secret number or the client card through the financial company server 16, the electronic authentication engine 20 issues a pertinent account code and a secret number...

17/3K/9 (Item 7 from file: 349) Links

PCT FULLTEXT

(c) 2007 WIPO/Thomson. All rights reserved.

00835725

OPTICAL PAYMENT TRANSCEIVER AND SYSTEM USING THE SAME

TRANSCEPTEUR DE PAIEMENTS OPTIQUE ET SYSTEME UTILISANT LE TRANSCEPTEUR

Patent Applicant/Patent Assignee:

HAREX INFOTECH INC; 16-6, Pil-dong 2-ga, Jung-gu, Seoul 100-272

KR; KR(Residence); KR(Nationality)

(For all designated states except: US)

PARK Kyung Yang; 202, Sinjoongang Villa, 8-1 Shingyo-dong, Jongro-gu-, Seoul 110-032

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

KIM Chul Ki; 309-1502, Kyonghyang Apt., Yatap-dong, Bundang-gu, Songnam-city, Gyonggi-do 463-924

KR: KR(Residence); KR(Nationality)

(Designated only for: US)

• 'HWANG Que Min; 206-502, 2nd Hyundai Apt., Gaepo-dong, Gangnam-gu, Seoul 135-808

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

JUNG Bong Sung; 101-1501, Hyundai Apt., 992 Daechi-dong, Gangnam-gu, Seoul 135-850

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

SUNG Kwang Hyun; 685-121, Jongrung 3-dong, Songbuk-gu, Seoul 136-850

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

KIM Do Ha; 196-1, Seokgwan-dong, Songbuk-gu, Seoul 136-818

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

JUNG Hoon Joon; 202, Hwaseong Town, 835-48 Dang-dong, Gunpo-city, Gyonggi-do 435-010

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

• KANG Bog Heui; 1-1204, Seoul Garden Apt., 555 Dobong 1-dong, Dobong-gu 132-751

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

• CHO Eun Sang; 22-87, Hyehwa-dong, Jongro-gu 110-530

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

• KIM Won Dong; 106-107, Hyundai Apt., 270 Hagye 2-dong, Nowon-gu, Seoul 139-873

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

• KIM Dae Yeon; 204-901, 2nd Hyundai Apt., 863-1 Banghwa 1-dong, Gangseo-gu, Seoul 157-857

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

• CHANG Kwang Su; 24-1, #545, Kuro 5-dong, Kuro-gu, Seoul 152-861

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

• WOO Hee Gu; 301, #8-100, Eungam 1-dong, Unpyong-gu, Seoul 122-905

KR; KR(Residence); KR(Nationality)

(Designated only for: US)

Patent Applicant/Inventor:

PARK Kyung Yang

202, Sinjoongang Villa, 8-1 Shingyo-dong, Jongro-gu-, Seoul 110-032; KR; KR(Residence); KR(Nationality); (Designated only for: US)

• KIM Chul Ki

309-1502, Kyonghyang Apt., Yatap-dong, Bundang-gu, Songnam-city, Gyonggi-do 463-924; KR; KR(Residence); KR(Nationality); (Designated only for: US)

• HWANG Que Min

206-502, 2nd Hyundai Apt., Gaepo-dong, Gangnam-gu, Seoul 135-808; KR; KR(Residence); KR(Nationality); (Designated only for: US)

• JUNG Bong Sung

101-1501, Hyundai Apt., 992 Daechi-dong, Gangnam-gu, Seoul 135-850; KR; KR(Residence); KR(Nationality); (Designated only for: US)

SUNG Kwang Hyun

685-121, Jongrung 3-dong, Songbuk-gu, Seoul 136-850; KR; KR(Residence); KR(Nationality); (Designated only for: US)

KIM Do Ha

196-1, Seokgwan-dong, Songbuk-gu, Seoul 136-818; KR; KR(Residence); KR(Nationality); (Designated only for: US)

• JUNG Hoon Joon

202, Hwaseong Town, 835-48 Dang-dong, Gunpo-city, Gyonggi-do 435-010; KR; KR(Residence); KR(Nationality); (Designated only for: US)

KANG Bog Heui

1-1204, Seoul Garden Apt., 555 Dobong 1-dong, Dobong-gu 132-751; KR; KR(Residence); KR(Nationality);

(Designated only for: US)

CHO Eun Sang

22-87, Hychwa-dong, Jongro-gu 110-530; KR; KR(Residence); KR(Nationality); (Designated only for: US)

KIM Won Dong

106-107, Hyundai Apt., 270 Hagye 2-dong, Nowon-gu, Seoul 139-873; KR; KR(Residence); KR(Nationality); (Designated only for: US)

• KIM Dae Yeon

204-901, 2nd Hyundai Apt., 863-1 Banghwa 1-dong, Gangseo-gu, Seoul 157-857; KR; KR(Residence); KR(Nationality); (Designated only for: US)

CHANG Kwang Su

24-1, #545, Kuro 5-dong, Kuro-gu, Seoul 152-861; KR; KR(Residence); KR(Nationality); (Designated only for: US)

• WOO Hee Gu

301, #8-100, Eungam 1-dong, Unpyong-gu, Seoul 122-905; KR; KR(Residence); KR(Nationality); (Designated only for: US)

Legal Representative:

• JO Eui Je(agent)

Top Patent & Law Firm, RM. 1405, Hyechun Building, #831 Yuksam-dong, Gangnam-gu, Seoul 135-080; KR;

	Country	Number	Kind	Date
Patent	WO	200169346	A2-A3	20010920
Application	WO	2001KR428		20010316
Priorities	KR	200013426		20000316
	KR	200026621		20000518
	KR	200031567		20000609
	KR	200016328 U		20000609
	K·R	200032454		20000613
	KR	200032455		20000613
	KR	200033198		20000616
	KR	200021614 U		20000728
	KR	200073716		20001206
	KR	200073717		20001206
	KR	200073718		20001206
	KR	200073719		20001206
	KR	20011540		20010111

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;

GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GW; ML;

MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;

UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

	IPC	Level
G06F-017/60		

Publication Language: English Filing Language: Korean Fulltext word count: 45154

Detailed Description:

...a decoding algorithm without keeping a separate encryption key in custody, and decodes the card information by using the received secret number (step 248). Thereafter, like the existing banking transaction systems... ... of a portable terminal. For the time when a person tries to find out a secret number illegally, the possessor of the portable terminal reports the loss of the portable ten-ninal, and thus it is not possible to find out a settlement secret number without having an agreement of the portable terminal possessor, except for the time when an afterservice (A/S) is applied. Also, if the settlement secret number is altered and then A/S is committed, even in the case of the A... ...the portable terminal is designed so that only one-time settlement is made and the secret number is again requested during reuse. In this case, the present invention can improve inconveniences greatly...commerce uses a settlement system requiring a user to input card information such as a user name, card number, secret number, and a valid date on a browser provided by a cyber shopping mall. The present... ...products. Then, the customer determines purchase items and makes up an order sheet. Then, the customer selects a settlement method for settlement of a debt on a screen and clicks the selected settlement method (step 591). The shopping mall system 584 checks if the customer's selected settlement method is an optical payment settlement method (step 592). If the customer determines the payment by one of other settlement method other than the optical payment, a....methods other than the optical payment. If a payment is an optical payment settlement, a customer uses a portable unit 581 which is an optical payment unit and transmits the card... ... optical payment unit has been described above, the detailed description thereof will be omitted. The customer inputs a secret number which is known only by him or her and presses a settlement button, and then...exit mode, the visitor manipulates a keypad on the portable terminal 800 and inputs a secret number in response to a request for an input of the secret number (step 812... portable terminal 830A checks if the secret number is correct (step 902). If the secret. number is correct, the portable terminal 830A displays the screen asking a transfer object as shown... ... can be embodied. In the case of a large amount of credit transaction requiring a secret number, a receiver receives a secret number and uses the same. Accordingly, there is no risk of leaking personal payment information. Also ... exit security system requiring personal identification as well as the financial transaction. In addition, a secret number and bio-identification data are combined when an in-person is identified in order to access payment information incorporated in a portable terminal. Thus, an...

Claims:

...optical payment transmitter of claim 46, further comprising a tone recognition module for recognizing the **secret** number from a tone signal generated in correspondence to the secret number input via a keypad...information into the

portable terminal together

with a settlement secret number; (c) inputting the secret **number** into the portable terminal during performing - 114 transactions and selecting a settlement mode; (d) transmitting both the card **information** and the **secret number** input into the portable terminal in the form of an optical signal, at the settlement mode; (e) receiving the card **information** and the **secret number** in the form of the optical signal and decoding the card **information** using the received **secret number**; and (f) performing a settlement operation with the decoded card information.

74 The security enhancement...

17/3K/10 (Item 8 from file: 349) Links

PCT FULLTEXT

(c) 2007 WIPO/Thomson. All rights reserved.

00826098

A NETWORK-BASED SYSTEM

SYSTEME BASE SUR UN RESEAU

Patent Applicant/Patent Assignee:

• INTERNET PAYMENTS PATENTS LIMITED; "Elsinore", Meath Road, Bray, County Wicklow

IE; IE(Residence); IE(Nationality) (For all designated states except: US)

• FORAN John Anthony; "Elsinore", Meath Road, Bray, County Wicklow

IE; IE(Residence); IE(Nationality)

(Designated only for: US)

• CORCORAN Joseph Patrick; 9 Carysfort Grove, Blackrock, County Dublin

IE; IE(Residence); IE(Nationality)

(Designated only for: US)

Patent Applicant/Inventor:

• FORAN John Anthony

"Elsinore", Meath Road, Bray, County Wicklow; IE; IE(Residence); IE(Nationality); (Designated only for: US)

• CORCORAN Joseph Patrick

9 Carysfort Grove, Blackrock, County Dublin; IE; IE(Residence); IE(Nationality); (Designated only for: US)

Legal Representative:

• O'CONNOR Donal H(et al)(agent)

Cruickshank & Co., 1 Holles Street, Dublin 2; IE;

	Country	Number	Kind	Date
Patent	WO	200159635	Αl	20010816
Application	WO	2001IE22		20010212

20000211 2000121 Priorities ΙE

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;

GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GW; ML;

MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;

UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	Level
G06F-017/60	Main

Publication Language: English Filing Language:

English

Fulltext word count:

12001

Detailed Description:

...next sequential number and does not have to be, in 3 0 any way, a secret number.

In step 1 10, the customer computer sends to the customer account server, the same information. This is a security procedure such that if the customer computer...

```
Description
Set
        Items
                S COMPUTER? ? OR CPU? ? OR CENTRAL() PROCESSING OR PROCESSOR? ? OR SERVER?
Sl
      6085819
? OR MINICOMPUTER? ? OR MICROCOMPUTER? ? OR PC OR LAPTOP? ? OR HANDHELD? ? OR NOTEBOOK? ?
OR COMPUTING OR MAINFRAME? ? OR MAIN()(FRAME OR FRAMES) OR SYSTEM? ? OR SELF()SERVIC? OR
ATM OR ATMS OR ((AUTOMATED OR AUTOMATIC)()(TELLER OR TRANSACTION OR SERVICE) OR CASH OR
MONEY OR BANK) (W) (MACHINE? OR TERMINAL? ?) OR ELECTRONIC() TELLER? ?
                S VIRTUAL OR ONLINE OR ON()LINE OR INTERNET OR NET OR WEB OR WWW OR CYBER
      1510501
OR ELECTRONIC OR WEBSITE? OR WEBPAGE? OR WEB()(SITE? OR SERVER? ?)
                ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNSPECIF? OR
       281445
UNKNOWN OR ?NO? (2N) (PERSONAL OR USER) FROM 2, 35, 65, 99, 139, 474, 475, 583
                S S3(5N)(DATA OR DEMOGRAPHIC? ? OR INFORMATION OR NUMBER? ? OR
        25839
IDENTIFICATION OR NAME? ? OR ID)
                S PASSWORD OR PIN OR PERSONAL()(IDENTIFICATION OR ID)()NUMBER OR CODE OR
       593439
KEY OR (PASS OR SECRET)()(WORD? ? OR PHRASE? ? OR NUMBER? ?) OR PASSPHRASE OR PASSNUMBER
OR (SECURITY OR ACCESS)()(CODE? ? OR KEY? ?) OR USER()(ID OR IDENTIFICATION OR NAME)
                S LOGON OR LOGIN OR (LOG OR LOGG? OR SIGN OR SIGNING OR SIGNED) () (IN OR
ON) OR AUTHENTICAT? OR (UNIQUE OR UNCOMMON OR DISTINGUISHING OR
DISTINCTIVE) (10N) (INFORMATION OR DATA OR STATISTIC? ? OR NUMBER? ?)
                S PATRON? ? OR CUSTOMER? ? OR CLIENT? ? OR USER? ? OR SUBSCRIBER? ? OR
ENROLEE? ? OR PARTICIPANT? ? OR PARTICIPAT?R? ? OR PERSON? ? OR DRIVER? ? OR OPERATOR? ?
(5N) GENERAT ??? OR ACCOMPLISH? OR BRING() ABOUT OR CREATE? OR FORM? ? OR INITIAT?
                S TRANSACTION? ? OR ORDER? ? OR PROCEDURE? ? OR INTERACTION? ? OR DEALING?
S8
      5729960
? OR ACTION? ? OR TRADE? ? OR TRADING OR PURCHAS??? OR EXCHANG??? OR DEAL? ? OR SELL??? OR
SALE? ? OR BUY???
                S S1(S)S4
S9
         5096
                S S2(S)S4
S10
         1224
                S S7(S)S5
S11
       111250
                S S7(S)S6
        12439
S12
                S S7(S)(S5 AND S6)
S13
          3474
                S (S1 OR S2)(S)S4
S14
         5746
                S S13(S)S14
S15
            79
                S S15(S)S8
            20
S16
                 S S4(S)(S5 OR S6)
          1379
S17
           496
                 S S17(S)S7
S18
                 S S18(S)(S1 OR S2)
S19
           303
                 S S18(S)S1
           274
S20
                 S S18(S)S2
            82
S21
                 S S20(S)S8
            82
S22
                 S S21(S)S8
            25
S23
                 S S22 OR S23
S24
            86
                 S S24 NOT PY>1998
            42
S25
                     (unique items)
            38
                 RD
S26
  ; show files
```

[File 2] INSPEC 1898-2007/Jan W4

(c) 2007 Institution of Electrical Engineers. All rights reserved.

[File 35] Dissertation Abs Online 1861-2007/Jan

(c) 2007 ProQuest Info&Learning. All rights reserved.

[File 65] Inside Conferences 1993-2007/Feb 05

(c) 2007 BLDSC all rts. reserv. All rights reserved.

[File 99] Wilson Appl. Sci & Tech Abs 1983-2007/Jan

(c) 2007 The HW Wilson Co. All rights reserved.

[File 139] EconLit 1969-2007/Jan

(c) 2007 American Economic Association. All rights reserved.

[File 474] New York Times Abs 1969-2007/Feb 06

(c) 2007 The New York Times. All rights reserved.

[File 475] Wall Street Journal Abs 1973-2007/Feb 06

(c) 2007 The New York Times. All rights reserved.

[File 583] Gale Group Globalbase(TM) 1986-2002/Dec 13

(c) 2002 The Gale Group. All rights reserved.

*File 583: This file is no longer updating as of 12-13-2002.

26/3,K/2 (Item 2 from file: 2) **Links**

Fulltext available through: SpringerLink USPTO Full Text Retrieval Options SCIENCEDIRECT

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved:

07109244 INSPEC Abstract Number: B9901-6120D-032, C9901-1260C-033 Title: Zero-knowledge authentication scheme with secret key exchange

Author Brandt, J.; Damgard, I.; Landrock, P.; Pedersen, T.

Author Affiliation: Dept. of Math. & Comput. Sci., Aarhus Univ., Denmark

Journal: Journal of Cryptology vol.11, no.3 p. 147-59

Publisher: Springer-Verlag,

Publication Date: Summer 1998 Country of Publication: USA

CODEN: JOCREQ ISSN: 0933-2790

SICI: 0933-2790(199822)11:3L.147:ZKAS;1-U Material Identity Number: M605-98003

Language: English Subfile: B C

Copyright 1998, IEE

Abstract: ...which is then modified (at no extra communication cost) into an identification scheme with secret key exchange for subsequent conventional encryption. Implemented on a standard 32-bit chip or similar, the whole protocol, which involves mutual identification of two users, exchange of a random common secret key and verification of certificates for the public keys (RSA, 512 bits), takes less than 3...

26/3,K/3 (Item 3 from file: 2) **Links**

Fulltext available through: <u>USPTO Full Text Retrieval Options</u> <u>SCIENCEDIRECT</u>

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved. 07105074 INSPEC Abstract Number: C9901-6130S-046

Title: Two integrated schemes of user authentication and access control in a distributed computer network

Author Jan, J.-K.; Tseng, Y.-M.

Author Affiliation: Inst. of Appl. Math., Nat. Chung-Hsing Univ., Taichung, Taiwan Journal: IEE Proceedings-Computers and Digital Techniques vol.145, no.6 p. 419-24

Publisher: IEE.

Publication Date: Nov. 1998 Country of Publication: UK

CODEN: ICDTEA ISSN: 1350-2387

SICI: 1350-2387(199811)145:6L.419:ISUA;1-3 Material Identity Number: B492-98006

U.S. Copyright Clearance Center Code: 1350-2387/98/\$10.00

Language: English

Subfile: C

Copyright 1998, IEE

Abstract: ...the scale of network technologies, security has become a major concern and a limiting factor.

Computer networks provide convenient procedures for users operating at remote places. However, an intruder can easily access and intercept information transmitted in an open channel. Two integrated schemes for user authentication and access control are proposed, which are mechanisms used to provide for the protection of... ...provides an efficient updating process for the modification of access rights. The second scheme allows servers to

simplify verification processes for multiple access requests of a user at the same time. Both schemes are

noninteractive approaches in which security is based on... ...more secure and efficient and suitable for applications in a distributed environment. Intruders cannot derive secret information from public information. Intruders are not able to acquire the passwords of users from previously intercepted messages. By applying a time stamp, the schemes can withstand the replaying...

26/3,K/4 (Item 4 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

06787710 INSPEC Abstract Number: B9802-6250F-031, C9802-5620-006

Title: Achieving user privacy in mobile networks Author Askwith, B.; Merabti, M.; Qi Shi; Whiteley, K.

Author Affiliation: Distr. Multimedia Syst. Group, Liverpool John Moores Univ., UK

Conference Title: Proceedings. 13th Annual Computer Security Applications Conference (Cat. No.97TB100213)

p. 108-16

Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA

Publication Date: 1997 Country of Publication: USA x+288 pp. ISBN: 0 8186 8274 4 Material Identity Number: XX97-03160 U.S. Copyright Clearance Center Code: 0 8186 8274 4/97/\$10.00

Conference Title: Proceedings 13th Annual Computer Security Applications Conference

Conference Sponsor: Appl. Comput. Security Associates; ACM Special Interest Group on Security, Audit, and

Control

Conference Date: 8-12 Dec. 1997 Conference Location: San Diego, CA, USA

Language: English Subfile: B C

Copyright 1997, IEE

Abstract: Third generation mobile networks aim to offer 'any service, anywhere, at any time'. Users require privacy within these systems in order to feel confident of their use. Privacy requirements (in mobile networks) are: content, location and identification privacy, and authentication. Differing from previous approaches to privacy, the network itself is considered to be an untrusted party. The paper proposes a scheme that allows the user to register with the network and remain anonymous (both location and identification). Digital mixes are used to create anonymity and authentication is achieved through a token based scheme. Finally the aspect of information leaking to authorised... ... is discussed and billing requirements are detailed which involve the use of 'coin' like tokens traded for services.

26/3,K/11 (Item 11 from file: 2) **Links**

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

05764266 INSPEC Abstract Number: B9410-6120B-155, C9410-6130S-054

Title: Multisecret threshold schemes

Author Jackson, W.; Martin, K.M.; O'Keefe, C.M.

Author Affiliation: Dept. of Pure Math., Adelaide Univ., SA, Australia

p. 126-35

Editor(s): Stinson, D.R.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1994 Country of Publication: West Germany x+491 pp.

ISBN: 3 540 57766 1

Conference Title: Proceedings of Crypto '93

Conference Date: 22-26 Aug. 1993 Conference Location: Santa Barbara, CA, USA

Language: English Subfile: B C

Abstract: A threshold scheme is a system that protects a secret (key) among a group of participants in such a way that it can only be reconstructed from the joint information held by some predetermined number of these participants. We extend this problem to one where there is more than one secret that participants can reconstruct

participants. We extend this problem to one where there is more than one secret that participants can reconstruct using the information that they hold. In particular we consider the situation where there is a secret s/sub K/ associated with each k-subset K of participants and s/sub K/ can be reconstructed by any group of t participants in K (t<or=k). We establish bounds on the minimum amount of information that participants must hold in order to ensure that up to omega participants (0<or= omega <or=n-k+t-1) cannot obtain any information about a secret with which they are not associated. We also discuss examples of systems that satisfy this bound.

26/3,K/14 (Item 14 from file: 2) Links

Fulltext available through: <u>USPTO Full Text Retrieval Options</u> <u>SCIENCEDIRECT</u>

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

05237511 INSPEC Abstract Number: A9220-4250-014, C9210-6130S-026

Title: Experimental quantum cryptography

Author Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J.

Author Affiliation: IBM Res., Yorktown Heights, NY, USA

Journal: Journal of Cryptology vol.5, no.1 p. 3-28

Publication Date: 1992 Country of Publication: USA

CODEN: JOCREQ ISSN: 0933-2790

Language: English Subfile: A C

Abstract: The authors describe results from an apparatus and protocol designed to implement quantum key distribution, by which two users, who share no secret information initially: (1) exchange a random quantum transmission, consisting of very faint flashes of polarized light; (2) by subsequent... ...small enough, distill from the sent and received versions a smaller body of shared random information, which is certifiably secret in the sense that any third party's expected information on it is an exponentially small fraction of one bit. Because the system depends on the uncertainty principle of quantum physics, instead of the usual mathematical assumptions such as the difficulty of factoring, it remains secure against an adversary with unlimited computing power.

26/3,K/22 (Item 22 from file: 2) Links

Fulltext available through: ScienceDirect (Elsevier) USPTO Full Text Retrieval Options SCIENCEDIRECT INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

03980331 INSPEC Abstract Number: C87061257

Title: TRASEC: Belgian security system for electronic funds transfers

Author van Heurck, P.

Author Affiliation: Centre for Interbank Res. in Informatics, Brussels, Belgium

Journal: Computers & Security vol.6, no.3 p. 261-8

Publication Date: June 1987 Country of Publication: Netherlands

CODEN: CPSEDU ISSN: 0167-4048

U.S. Copyright Clearance Center Code: 0167-4048/87/\$3.50

Language: English

Subfile: C

Abstract: The Belgian banking community has designed a standard security system TRASEC (transmission security) for EFT (electronic funds transfer) between corporate customers and all financial institutions, which will become operational by the end of 1987. TRASEC ensures the integrity and authentication of EFT in an automated environment and is easily integrated in the actual banking procedures. The system is independent of the transfer medium, the application, and the configuration and type of the computers of the customer and the financial institution. The customer's system consists of a condensing module and an authentication module. The condensing module is a one-way-function, implemented as a program on the customer's computer, which condenses a transfer file to a digest. The digest is the input of the authentication module, which calculates a digital signature (MAC). This authentication module is a smart card which contains the message authentication algorithm based on DES, password management, secret keys, passwords, sequence number, etc.

26/3,K/23 (Item 23 from file: 2) Links

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

03832532 INSPEC Abstract Number: C87017890

Title: Electronic seal for protection of electronic money in Sweden, Finland and Norway

Author Linden, C.

Author Affiliation: SAKdata AB, Ingejorscentrum, Sollentuna, Sweden

Conference Title: Proceedings of the 1986 International Carnahan Conference on Security Technology: Electronic

Crime Countermeasures p. 135-40

Editor(s): Jackson, J.S.

Publisher: Univ. Kentucky, Lexington, KY, USA

Publication Date: 1986 Country of Publication: USA 255 pp.

ISBN: 0 89779 066 9

Conference Sponsor: IEEE; Chalmers Univ. Technol; Univ. Kentucky; GTE Service Corp.; Nat. Swedish Board

Tech. Dev

Conference Date: 12-14 Aug. 1986 Conference Location: Gothenburg, Sweden

Language: English

Subfile: C

Abstract: ...for detection of any criminal changes in transmission or storage of valuable information, called the electronic seal, is being used by banks and corporations in Sweden. The electronic seal is a software algorithm with cryptological qualities that calculates a security total combining information to be protected with a unique, secret key. The protected information remains in clear (legible) text. Swedish banks are using the method to protect 80 million electronic interbank clearing transactions annually and major insurance companies in Sweden give their clients a 10% discount on their computer crime policies provided the client corporations have secured their electronic payments by the electronic seal. The seal software has been integrated, as a security feature, into many standard packages...

26/3,K/24 (Item 24 from file: 2) Links

Fulltext available through: USPTO Full Text Retrieval Options SCIENCEDIRECT

INSPEC

(c) 2007 Institution of Electrical Engineers. All rights reserved.

02895964 INSPEC Abstract Number: C82031448

Title: Pin protection/verification for electronic funds transfer

Author Lennon, R.E.; Matyas, S.M.; Meyer, C.H. Author Affiliation: IBM Corp., Armonk, NY, USA

Journal: IBM Technical Disclosure Bulletin vol.24, no.7B p. 3906-9

Publication Date: Dec. 1981 Country of Publication: USA

CODEN: IBMTAA **ISSN:** 0018-8689

Language: English

Subfile: C

Abstract: A protocol method is disclosed for point of sale (POS) terminals (T) connected to a host (H) system such that when a transaction is initiated an assigned secret customer personal identification number (PIN), which is used to identify the customer, can be verified at either T or H having the benefit of cryptographic protection

during...

26/3,K/38 (Item 8 from file: 583) **Links**

Gale Group Globalbase(TM)

(c) 2002 The Gale Group. All rights reserved.

04540682

ICI standardises on software from German SAP

UK - ICI TO STANDARDISE ON SOFTWARE FROM SAP

Computer Weekly (CRW) 19 September 1991 p64

ISSN: 0010-4787

...chemical manufacturer, is to standardise worldwide on integrated software products from SAP (Germany), an IBM mainframe software house, in response to global market requirements. The deal is likely to account for a large part of the GBP130 mil that ICI will spend on its Information Services division in 1991. A SAP client for 19 years, ICI has made a commitment to move all transaction processing operations to the company's R2 software system. As a result of ICI's decision, its seven worldwide businesses, including pharmaceuticals, agrochemicals, industrial chemicals and explosives, must use SAP for transaction processing. At present the deal applies to ICI's European and US arms, and is still just a 'tactical' solution... ...integrated nature of SAP is preferable to the interfaced software of such rival offerings as Computer Associates or Dun & Bradstreet software and is also much easier to use in real time mode. ICI is also developing a common systems architecture and common data definition for controlling key levels of data worldwide. An unspecified number of ICI IT staff will lose their jobs as a result of the SAP deal.**

26/6/1 (Item 1 from file: 2) Links

07126842 INSPEC Abstract Number: A1999-03-2921-038, C1999-02-7320-048

Title: Beam optics - a program for analytical beam optics

Publication Date: 6 Aug. 1998

Copyright 1999, IEE

26/6/2 (Item 2 from file: 2) Links

07109244 INSPEC Abstract Number: B9901-6120D-032, C9901-1260C-033

Title: Zero-knowledge authentication scheme with secret key exchange

Publication Date: Summer 1998

Copyright 1998, IEE

26/6/3 (Item 3 from file: 2) **Links**

07105074 INSPEC Abstract Number: C9901-6130S-046

Title: Two integrated schemes of user authentication and access control in a distributed computer network

Publication Date: Nov. 1998

Copyright 1998, IEE

26/6/4 (Item 4 from file: 2) Links

06787710 INSPEC Abstract Number: B9802-6250F-031, C9802-5620-006

Title: Achieving user privacy in mobile networks

Publication Date: 1997 Copyright 1997, IEE

26/6/5 (Item 5 from file: 2) Links

06733235 INSPEC Abstract Number: B9712-6250F-050, C9712-7410F-028

Title: Development of the home location register/authentication center in the CDMA mobile system

Publication Date: Oct. 1997

Copyright 1997, IEE

26/6/6 (Item 6 from file: 2) Links

06565161 INSPEC Abstract Number: B9706-6150M-012, C9706-5640-004

Title: Designing a virtual access control configuration protocol for implementation over ISDN and

shared-media networks Publication Date: 1996 Copyright 1997, IEE

26/6/7 (Item 7 from file: 2) Links

06507034 INSPEC Abstract Number: B9704-6230-005, C9704-6130S-014

Title: A proposal for security services in ATM networks

Publication Date: 1996 Copyright 1997, IEE

26/6/8 (Item 8 from file: 2) Links

06442780 INSPEC Abstract Number: B9701-6250G-023, C9701-7190-020 Title: Auctioning by satellite using trusted third party security services

Publication Date: 1995 Copyright 1996, IEE

26/6/9 (Item 9 from file: 2) Links

05898758 INSPEC Abstract Number: C9504-0220-031

Title: Classroom guidelines on program documentation and formatting

Publication Date: Winter 1995

Copyright 1995, IEE

26/6/10 (Item 10 from file: 2) Links

05795714 INSPEC Abstract Number: B9411-6140-400, C9411-5260-148 Title: Symbolic match hypothesis evaluation for UHRR radar targets

Publication Date: 1994

26/6/11 (Item 11 from file: 2) Links

05764266 INSPEC Abstract Number: B9410-6120B-155, C9410-6130S-054

Title: Multisecret threshold schemes

Publication Date: 1994

26/6/12 (Item 12 from file: 2) Links

05629564 INSPEC Abstract Number: C9405-7140-023

Title: Maintaining patient confidentiality in an electronic world

Publication Date: Feb. 1994

26/6/13 (Item 13 from file: 2) Links

05365270 INSPEC Abstract Number: C9304-6110J-020

Title: Domain model-driven software reengineering and maintenance

Publication Date: Jan. 1993

26/6/14 (Item 14 from file: 2) Links

05237511 INSPEC Abstract Number: A9220-4250-014, C9210-6130S-026

Title: Experimental quantum cryptography

Publication Date: 1992

26/6/15 (Item 15 from file: 2) Links

05165423 INSPEC Abstract Number: C9207-7160-032

Title: Production management systems for one-of-a-kind products

Publication Date: April 1992

26/6/16 (Item 16 from file: 2) Links

05128196 INSPEC Abstract Number: C9205-6130S-043

Title: TRASEC: national security system for EFTS in Belgium

Publication Date: 1991

26/6/17 (Item 17 from file: 2) Links

04843048 INSPEC Abstract Number: B91019606, C91023120

Title: An integrated Data Protection Scheme in a Distributed Computing environment

Publication Date: 1990

26/6/18 (Item 18 from file: 2) **Links**

04783000 INSPEC Abstract Number: B91003793, C91003987

Title: Superdistribution: the concept and the architecture

Publication Date: July 1990

26/6/19 (Item 19 from file: 2) Links

04372345 INSPEC Abstract Number: C89034193

Title: The TRASEC system for EFT in Belgium: a case study

Publication Date: 1988

26/6/20 (Item 20 from file: 2) Links

04236034 INSPEC Abstract Number: B88066308, C88058349

Title: How to insure that data acquired to verify treaty compliance are trustworthy

Publication Date: May 1988

26/6/21 (Item 21 from file: 2) Links

04160364 INSPEC Abstract Number: C88041786

Title: Turbo Rand: Monte Carlo sampling and simulations

Publication Date: March 1988

26/6/22 (Item 22 from file: 2) Links

03980331 INSPEC Abstract Number: C87061257

Title: TRASEC: Belgian security system for electronic funds transfers

Publication Date: June 1987

26/6/23 (Item 23 from file: 2) **Links**

03832532 INSPEC Abstract Number: C87017890

Title: Electronic seal for protection of electronic money in Sweden, Finland and Norway

Publication Date: 1986

26/6/24 (Item 24 from file: 2) Links

02895964 INSPEC Abstract Number: C82031448

Title: Pin protection/verification for electronic funds transfer

Publication Date: Dec. 1981

26/6/25 (Item 25 from file: 2) Links

02834876 INSPEC Abstract Number: B82021480, C82015346

Title: Some cryptographic principles of authentication in electronic funds transfer systems

Publication Date: Oct. 1981

26/6/26 (Item 26 from file: 2) Links

02708802 INSPEC Abstract Number: B81033423

Title: The wiretap channel with feedback

Publication Date: 1981

26/6/27 (Item 1 from file: 35) Links

01807963 ORDER NO: AADAA-19939409

Intelligent support for engineering collaboration

Year: 1998

26/6/28 (Item 2 from file: 35) **Links**

01598588 ORDER NO: AAD98-00347

ITERATIVE DECODING (DECODERS, CODE CONSTRUCTION)

Year: 1997

26/6/29 (Item 3 from file: 35) **Links**

01496441 ORDER NO: NOT AVAILABLE FROM UNIVERSITY MICROFILMS INT'L.

ASPECTS OF GROUP COMMUNICATIONS SECURITY (CRYPTOGRAPHY, SECRET SHARING)

Year: 1995

26/6/30 (Item 1 from file: 474) Links

00342754 NYT Sequence Number: 107324721124

(New rules of evidence issued for Fed ct system by Sup Ct in past wk establishes 'secret of state' system that denies cts access to information whose disclosure Govt regards as 'contrary to the public interest'; code was largely drafted by advisory com of US Judicial Conf headed by A E Jenner Jr and was officially promulgated by Sup Ct to go into effect July 1 if Cong does not take any contrary action; other new proposals likely to arouse controversy in Cong include granting Govt privilege to refuse to give evidence and to prevent any person from giving evidence if it is likely that testimony might reveal 'secret of state' or lesser category of 'official information'; such secret of state is defined as Govt secret relating to 'natl defense or the internatl relations of the US' while official information is any Govt information whose disclosure 'is shown contrary to the public interest'; such privileges could be invoked by adm in freedom of information cases brought in Fed cts to obtain access to Govt documents in which citizens believe they have legitimate interest)

Friday November 24 1972

26/6/31 (Item 1 from file: 583) Links

06597966

Ssb e Banca Antonveneta lanciano i pagamenti sicuri sul Web con Visa

ITALY: ELECTRONIC TRANSACTIONS SECURE WITH VISA

26/6/32 (Item 2 from file: 583) Links

06417846

Toshiba gets smarter

JAPAN: SAFER SMARTCARD TO BE LAUNCHED BY TOSHIBA 14 Jan 1997

26/6/33 (Item 3 from file: 583) Links

06365914

La carte tZlZphonique s'affranchit de la puce

FRANCE: INTERCALL'S NEW CARD 13 Sep 1996

26/6/34 (Item 4 from file: 583) Links

06119957

Four telecom firms to share the 500,000 GSM mobile phones mkt

TAIWAN: NT, MOTOROLA ETC TO SUPPLY GSM MOBILES 24 Feb 1995

26/6/35 (Item 5 from file: 583) **Links**

06033006

Junge Kunden greifen gern zum Hoerer

GERMANY: TELEBANKING CUSTOMERS ON THE RISE

11 Aug 1994

26/6/36 (Item 6 from file: 583) **Links**

05680217

KREDITVERGABE BIETET DEM HANDEL EINE NEUE VARIANTE VON ELECTRONI

GERMANY - NEW EPOS PAYMENT SYSTEM 2 February 1993

26/6/37 (Item 7 from file: 583) **Links**

05488061

LIGHT UP THE NIGHT

FRANCE - EDF INTRODUCES NEW ELECTRICITY PAYMENT SYSTEM 9 December 1992

26/6/38 (Item 8 from file: 583) Links

04540682

ICI standardises on software from German SAP

UK - ICI TO STANDARDISE ON SOFTWARE FROM SAP 19 September 1991

Achieving User Privacy in Mobile Networks

Bob Askwith, Madjid Merabti, Qi Shi, Keith Whiteley
Distributed Multimedia Systems Group
Liverpool John Moores University
Byrom St, Liverpool, England, L3 3AF

e-mail: {R.ASKWITH, M.MERABTI, Q.SHI, K.WHITELEY}@livjm.ac.uk Web Site: http://www.cms.livjm.ac.uk/www/research/dms/dmsgroup.htm

Abstract

Third generation mobile networks aim to offer 'any service, anywhere, at any time'. User require privacy within these systems in order to feel confident of their use. Privacy requirements (in mobile networks) are: content, location, and identification privacy, and authentication. Differing from previous approaches to privacy, the network itself is considered to be an untrusted party.

This paper proposes a scheme that allows the user to register with the network and remain anonymous (both location and identification). Digital mixes are used to create anonymity and authentication is achieved through a token based scheme. Finally the aspect of information leaking to authorised third parties is discussed and billing requirements are detailed which involve the use of 'coin' like tokens traded for services.

1. Introduction

An exciting prospects for future computing is the requirements brought about by the demand for user mobility. The rapid growth of the cellular telephone markets during the last decade [1] has proved that users are demanding mobility. This has led to extensive research and development towards third generation mobile networks known as Universal Mobile Telecommunications System (UMTS) [2] in Europe and Future Public Land Mobile Telecommunication System (FPLMTS) [2] globally. The primary goal of such a network(s) is to provide the user with any service, anywhere, any time.

User mobility is seen as operating on two distinct levels, terminal and personal mobility. Terminal mobility allows a user to roam whilst carrying a network terminal, such as a mobile phone. Personal mobility on the other hand allows

the user to roam free of the terminal and connect to the network through any available terminal. Personal mobility is important since it allows the user to connect via specialised terminals that offer more advanced services, e.g. video conferencing, which may not be personally available. Alternatively it allows a user to connect to a network that a personal terminal may not be compatible with. Personal mobility is achieved through the carrying of a subscriber identity module (SIM) that holds sufficient details to enable connection to the network from any compatible terminal.

In order for these systems to become ubiquitous users need to be convinced that they provide an adequate level of security for their needs. This paper looks at the architecture for mobile networks (section 2), examines the requirements for user privacy in such networks (section 3), surveys the existing efforts in mobile security (section 4), and finally proposes some research to extend the current approaches which will then fulfil the users requirements (section 5).

2. Mobile Networks Architecture

This section provides some initial background to mobile networks followed by a brief description of the architecture of current mobile cellular networks.

The first mobile cellular networks in operation were the analog telephone systems. These are referred to as first generation mobile networks and had very low security (much press being given to cloning phones at the time). Second generation networks have appeared more recently and are based on digital cellular telephony. These systems, such as the Global System for Mobile Communications (GSM) in Europe [3], have considerably more security (encryption and authentication). Most recently the desire for global mobile computing systems has brought about

plans for UMTS (in Europe) and FPLMTS. These third generation networks are not limited to telephony and are aimed to provide a global mobile data network providing a secure 'anytime, anywhere, any service' capability.

In order to avoid the replacement of the existing hardware infrastructure it is planned that Intelligent Networks [4] concepts should be used. Intelligent Networks allows functionality to be built in to the network components such as routers. One of the major aims of Intelligent Networks is that new services can be developed quickly and cost effectively. An example of an Intelligent Network service is 'caller waiting'. It is proposed that the security features for mobile networks be provided through additional Intelligent Network services.

Mobile terminals in second generation networks (and proposed third generation networks), e.g. a mobile phone, operate by communicating with cells. These cells send and receive radio waves within a set frequency band (900Mhz for GSM). Each cell can handle a set number of channels within this range to allow for that number of simultaneous users within the cell. A cell may be able to pick up signals up to 1km, beyond which the next adjacent cell will handle the signals.

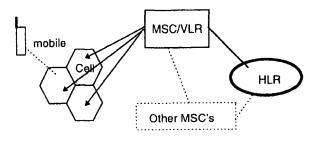


fig. 1. Cellular network infrastructure.

Cells are organised so that they form a hexagonal geographic reception structure as shown in figure 1. A collection of these cells, known as a location area, are controlled by a Mobile Switching Centre (MSC). Within the MSC are the routing capabilities and other hardware/software to handle mobile calls. The Intelligent Network software operates in the MSC and as such this is where some of the security features will lie.

Each MSC holds a visitor location register (VLR), a database of the current users in the area. Users are associated with a home location register (HLR) which stores a users profile. The functionality for call management (including security) is also held in the MSC and uses the VLR and HLR entries to track users.

When a user enters a new cell it must register with the VLR via the cell. If a user leaves a location area that users VLR entry must no longer have effect. When registering a user the VLR will notify the users HLR so that incoming calls can be routed to the correct MSC (and then cell) via the entry in the HLR/VLR. This problem is known as location management. Much research has been done in this area a recent summary of which can be found in [5].

3. Privacy Requirements for Mobile Networks

Privacy, the protection of data from unauthorised parties, has never been as important an issue as it is today. The range of applications and the value of data being transferred is continuously increasing. Press coverage of security breaches means that users are more aware of the issues than ever and consequently demand adequate security for their data.

Within networking environments there are many security measures. Fundamental to most of these is encryption, the coding of information using a digital key. Encryption can either be symmetric (secret key algorithms, e.g. DES [6]) or asymmetric (public key algorithms, c.g. RSA [7]). Encryption can be used to provide message content privacy and also to build protocols that satisfy other security requirements such as authentication (e.g. Kerberos [8]).

A number of research efforts have been targeted at understanding the requirements of mobile network security. A notable effort was by Federrath et al [9]. The authors discuss the security requirements for mobile networks and suggested ways of dealing with these. Their requirements are categorised into protection of confidentiality, integrity, and availability. Confidentiality is then categorised into content, location, and addressee privacy whilst integrity is categorised into content, addressee, and usage integrity. Availability is stated as the enabling of communications between parties who wish to and are able to communicate.

The main aim of this research is to achieve confidentiality and integrity requirements. As such a more pertinent way to categorise the requirements is to look at four separate types; content privacy, location privacy, identification privacy, and authentication.

• Content Privacy

The most basic of the requirements is content privacy, ensuring that the contents of a message arc secure from

unauthorised parties. A mobile terminal communicates with a cell via the air which is an inherently insecure medium. An eavesdropper can quite cheaply obtain scanning equipment which would enable them to listen to messages being transmitted.

Protection of message content is also required against the network itself as it too may be an unauthorised party. Users do not expect people to listen in on their business and even where a system such as key recovery [10] is in use, content privacy is fundamental to user data privacy.

Another aspect of content privacy is integrity. The receiver of a message must be convinced that the message is the same message as the one sent by the sender. Achieving message integrity will enable communicating parties to be sure that their messages have not been tampered with (even if the content remained unseen).

Location Privacy

The location of a mobile user should be untraceable to unauthorised parties, including the network. However, location data should be available in an efficient way to authorised parties.

As a mobile user roams around, the network must be able to route messages to that user. In order to do so location information must be available. However a mobile users location may be sensitive for many reasons. An example is where a user travels out of the country on holiday. The fact that a user is out of the country is a suggestion to a criminal that their house may be worth investigating for burglary.

The network should be denied access to this information to prevent the misuse of user data. Users in foreign networks might be particularly keen to have their location kept secret. Where this network is not their normal provider then it would imply that such a network is less trustworthy.

Authorised users may require location information for application purposes so it is desirable for the information to be available in an authenticated way. One such example may be a company service fleet co-ordination application. A company wishing to respond to service requests from customers would benefit from knowing the location of the nearest fleet vehicle to the customer.

Identification Privacy

The identification of mobile users should be private from unauthorised users, i.e. mobile users should be anonymous. Anonymity in mobile networks is considered necessary to prevent misuse of traffic information by third parties. The identification of users and terminals may be used by third parties to gather usage information for services etc. One such misuse may be the selling of access information to market research companies. Users desire that their activities are not monitored on a personal level. Again, as with location information, it may be desirable for authorised users to have access to identification for application purposes, under authenticated conditions.

Authentication

Authentication is the process of proving to a communicating party that you are who you say. Each time we type in our password into our office workstation we are authenticating ourselves to the local network. Mobile users must be able to authenticate themselves to the network and to other communicating parties. In addition, the network must be able to authenticate itself to a mobile user.

Authentication is required to establish trust between communicating parties. A network will only provide service if a mobile user is deemed authentic, in order to prevent fraudulent access. A mobile user should not accept connection to a network that cannot authenticate itself to the mobile user since the user cannot then be sure of the intentions of the unauthenticated network. For example a network may attempt to charge your home network for services that were not actually used.

4. Existing Solutions Towards Security and Privacy

A considerable amount of research effort has been put into the security of mobile networks. Much of this has been directed towards achieving content privacy and authentication in order to prevent fraudulent use of the networks. Unauthorised access to mobile networks is a serious issue for both networks and users and such fraud was estimated to be as high as \$500m in 1993 [11]. This section aims to investigate some research work relevant to the area and point out some remaining shortcomings.

Content Privacy

Our requirement for content privacy can be provided by encryption schemes such as DES [6] and RSA [7]. Typically a combination of the two types are used in order to aid performance. Secret-key systems are faster but require public-key systems initially to distribute keys.

Additionally, public-key systems can be used to achieve integrity through the use of digital signatures [12]. A digital signature is an encrypted code added to a message that allows the recipient to authenticate the sender. A sender signs a message by encrypting a code that is a function of the message with their secret key. A recipient decrypting this signature with the senders public key can be confident the sender is authentic, since only they could have produced the signature (being the only one knowing the secret 'signing' key). Signatures also provide message integrity as (if correct) they guarantee the message had not been altered between sender and recipient.

Authentication

A mobile user must be able to be authenticated by any part of the network, and as such by parts that have no prior knowledge of it (i.e. VLR's in foreign networks). In general, to achieve authentication, a three way protocol is used. The user is authenticated to the foreign network by the home network and likewise the foreign network is authenticated to the user by the users home network. Much research has been done in this area, some relevant works include [13-17].

Although these schemes provide adequate authentication in terms of gaining trust for the parties involved, and as such meet our requirements for authentication, they do not provide the required privacy for the users location and identification. In order to authenticate a user the identity is required and since the underlying network is not assumed to provide location privacy the location is revealed simply through the addressing of the messages.

Location and Identification Privacy

These two types of privacy work hand in hand. If a users identity is private, through a pseudonym, then location information is clearly of no use to an attacker.

There are several works in this area, most notably [17-19]. All of these use the concept of a digital mix as first introduced by Chaum in [20], and described here in 4.1. These works protect the user from third party attacks on location and identification but fail to do so from the network itself. Hoff's work in [18] does go some way towards doing this but fails to achieve this securely enough. Details of the problem of Hoff's work are discussed in 4.2.

4.1. Digital Mixes

A digital mix enables two parties to communicate without unauthorised parties being able to determine either the message content or the source and destinations of the messages. In addition, the sender of a message can remain anonymous to the recipient. In order to achieve this an intermediate computer called a 'mix' processes messages so that header information is hidden from following communications.

A user x, wishing to send a message to another user y, encrypts the message under the public key of y, attaches y's address and then encrypts this under the public key of the mix. The message then appears as an encrypted message addressed to the mix. The mix can then decrypt the message (leaving the message encrypted only under y's public key) and send it onto y. Messages are signed so that integrity of proof of sending is maintained.

There are several problems with this simplified explanation. First y cannot return a message since x's address is not known to y. Secondly, although the addresses are hidden, a third party could observe the input's and outputs to a mix and deduce from message sizes the end points of a communication. Finally the mix has access to the source and destination addresses thus creating a gap in the users anonymity.

The problem of return addressing is solved by the sender encrypting their address into their message using a key known only to the mix. The recipient will not be able to read the address but can hand the address back to the mix with a return message that will allow the mix to pass the message back to the original sender. An added bonus of return addresses is that these addresses can be used to certify mail. If the return address is sent back as part of the message then the original sender can mail this back to show that the message was received.

The problem of traceability is solved by the mix batching and reordering messages and making fixed length messages so that an eavesdropper cannot determine any correspondence about the input and outputs to a mix.

If several mix computers are used, each under a different authority then the problem of a mix using traffic information is solved unless all participants in the mix collaborate. Also the length of the mix will decrease the traceability. If a larger number of mixes are involved they are likely to be processing a larger number of messages thus making the batching process more efficient to perform.

An implementation of an anonymous remailer (BABEL) using digital mixes was detailed by Gulcu and Tsudik in [21]. This shows some interesting implications of Chaum's original paper [20]. Details are given on chaining mixes together to add confusion, using random detours within mix routes, making replies anonymous for broadcast messages, and decoys within message batches. This latter point helps to prevent an attacker from entering all but one of the messages into a batch and looking for the remaining message to be output from the mix. Although [21] is not directed at mobile networks it does offer some interesting applications of the digital mix that are relevant to any implementation within a mobile network.

Such an implementation would meet our requirements as far as providing location and identification privacy. However the static nature of such a mix means that the efficiency would vary depending on the location of the user using the mix. If a digital mix were to be used in a mobile environment then it must be offered as an independent service to the network. As such authentication of the user may be required for use of the mix. This implementation of a mix does not offer these features.

Perhaps the major drawback for the use of digital mixes is their potential inefficiency. To operate correctly they require the batching of messages. If used in an asynchronous messaging system then where delay was less important then this could be acceptable but in a system requiring real-time communication (e.g. multimedia data such as audio and video) any delay is undesirable. The implementation of any such mix would therefore have to be carefully thought out.

4.2. Hoff's Anonymous Subscriber System

Hoff's work in [18] protects the users location and identification information from third parties by the use of temporary identification numbers. When a user arrives in a cell and registers with the network a digital mix (see section 4.1) is used to prevent parts of the network from discovering the actual location. The network then stores the users international identification with the pseudonym in order to route messages. When the user is in a foreign network this means the home network does not know the actual location but can route messages to the foreign network for forwarding.

This work fails to protect the users information from the network where the user is within the local network since the pseudonym and identification when stored in this instance will simply be a reference to the users location. A user in a foreign network will be visible to the home

network as being in a foreign network (although the exact location remains unseen). These two points do not satisfy fully the requirements for location privacy which state that the network, in addition to external third parties, should not be able to determine the location and identification of the mobile user.

The use of a digital mix operated by the network is also not a sound proposal since collaboration of the mix and the network could lead to user information being revealed. Indeed it is not clear exactly how these mix nodes are integrated into the network. The operation of a mix in a foreign network cannot also be guaranteed. The privacy of user data should, as far as possible, be in the user's control and therefore, allowing the user to choose a mix setup would be highly preferable.

Finally although this paper addresses the problem of mobility management security no detail is given to the authentication problems of users moving into new areas. Whilst this has been dealt with by [13-17] protection of user location and identification data from the network itself is not, as mentioned, considered.

5. Proposed Research to Achieve User Privacy

We have seen that there have been many interesting research efforts towards achieving user privacy in mobile networking environments. Examination of these against the set of requirements outlined earlier in this paper revealed that there are a number of remaining deficiencies. This section proposes to extend the existing approaches in order to achieve full user privacy. This includes privacy from the network as well as from third parties. We close this section by looking at the problem of information leaking and billing for services.

5.1. Architecture

It is clearly infeasible to offer solutions that require extensive restructuring of the existing infrastructure. Any new methods should be implementable within the current network software architecture and any hardware additions should ideally be as minimal as possible.

We start by looking at the elements of the architecture that are affected by this research and then how these satisfy the requirements outlined earlier in the paper (section 3). Figure 2 shows the proposed architecture. A communicating mobile entity is composed of a user, a subscriber identity module (SIM) - smart card, and mobile communications terminal. This communicates with the local network, as detailed in section 2. In order for a

communication to occur a mix network is used between the local and home networks (which may be the same network). An external user may communicate directly with the chosen mix network once given a pseudonym for the user.

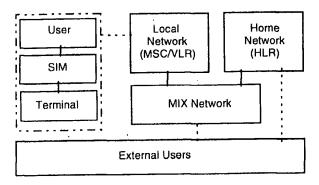


fig 2. Mobile Network Security Architecture.

The user carries with him/her a subscriber identity module (SIM) that holds personal account details and allows him/her to connect to the network from a terminal. A SIM is a smart card that can hold user information in a tamper proof way [22]. The SIM is inserted into a mobile terminal to enable personal communications. In this research it is required that the SIM contains a tamper proof public key pair. The private key of the key pair is only ever known to the SIM. This will allow the user to set up secure communications and achieve content privacy. A users public key should be available to any user wishing to communicate. This can be done by storing the key in the users home location register (HLR). If desired this could then be integrated into some key certification scheme, however this is considered outside the scope of this paper.

When a user roams around the network the network must keep track of the user in order to route messages. There are two distinct instances when the network will have to update location information. Firstly when a terminal is switched on or becomes active to the network again and secondly a user moving from one location to another. In each of these instances the user must register with the local mobile switching centre (MSC). Authentication must also take place between the three components (local MSC, home network, and user).

Registration starts by the user requesting authentication with the local network. In order to do this an authentication message is passed to the home network via a user designated digital mix. Upon receipt of this request the home network can then authenticate the user to the foreign network, and the foreign network to the user. As a

consequence of this registration the home network is provided with a pseudonym for the user by retaining the return address from the user.

The authentication process must maintain the privacy of the mobile user. The home network will obtain the identification of the user (in order to place an entry for in the HLR) but must not obtain the location. Authentication does not require location information so this is not a problem. Identification of the parties involved is more of a problem. To achieve authentication of the local network, this network must be identified. Identification of this network will reveal partial location information to the home network. Clearly this is undesirable.

An alternative authentication is thus required. When the user requests authentication the local network passes this request anonymously to the home network. The home network issues a challenge to the user via the local networks return address. The response to this is then passed back to the home network which allows the home network to reply to the local networks request for mobile user authentication.

Now that the user is authenticated to the local network the final step is for the local network to authenticate to the user. This is done by asking the local network to authenticate itself with the home network. The local network passes to the home network, via the mix address supplied by the user, an authentication request. This request identifies the local network. No connection is made with the user at this point. The home network now passes back a token to the local network which is produced via a blinding protocol as first devised by Chaum in [23]. This means that the token can be validated but not linked to a particular entity. This token is passed to the user terminal which can then submit the token back to the home network. The home network then checks the token and replies to the user accordingly.

At this point all three parties have been authenticated and the users HLR contains a pseudonym for routing messages to the users current MSC. The local network, convinced of the authenticity of the user, assigns a pseudonym to the user and places an entry into the visitor location register (VLR). When an incoming message appears for the user, the users home network routes the message through the digital mix to the users current MSC using the given return address. The MSC can then route messages to the user with given the pseudonym entry in the VLR.

To summarise, the following messages are used in the protocol (all messages between the local and home networks use the digital mix designated by the user in the initial request). The exact content of the messages and the encryption's upon each are the topic of future work and thus not covered here.

M = Mobile User; L = Local Network; H = Home Network:

1. M to L	Registration Request
2. L to H	M Authentication Request
3. H to M (via L)	Challenge for M
4. M to H (via L)	Response to Challenge
5. H to L	Authentication of M
6. L to H	L Authentication
7. H to M (via L)	Token for M
8. M to H (via L)	Token for L Authentication
9. H to M (via L)	Authentication of L

Communications are now approaching anonymous and untraceable based on the information known by each element of the network. It can of course, never be said to be 100% secure. The MSC knows only the pseudonym chosen by itself for the user and the address of the mix used by the user. Therefore, although it knows the location of the user, the real identification is not known. The digital mix can only determine that a message between two particular MSC's. The home network has no knowledge of the location of the user since it is only aware of the digital mix return address given in the registration process by the user. An end user attempting communication with a mobile user is only aware of that users real identification, the location remains unknown. Thus by unlinking location and identification from the elements of the network the user achieves privacy.

An attacker attempting to discover information could determine the identity of the mix used by the user by watching the output from the home network. The location of the user would be unobtainable to an attacker due to the untraceability created by the mix, assuming the mix network remains uncompromised.

It would thus be reasonable to allow an end user to cache the address of the mix for further communications. When the user becomes unreachable at their current location then the user can query the HLR for the new location and carry on as before. This would save communications being passed through the home network.

The digital mixes used in mobile networks must be operated independently of the mobile network service

provider. This will allow the user to choose a trustworthy mix supplier and make collusion of involved parties harder to achieve. To discover user information collusion would be required between the home network, the mix, and the current MSC of the user.

It is a major aim of this research to develop a mix that satisfies all the requirements laid out in this paper in a reliable and efficient way. As already noted it is questionable whether digital mixes are suitable for real time communications, a problem which needs seriously addressing. The distributed nature of mobile computing and the fact that a user could appear anywhere in the world means that the starting point of the mix needs to be as close to the user as possible. Some method of locating this needs to be found in order to prevent messages travelling unnecessary distances. Secondly a user subscribing to a mix will likely be charged in some way for such a service by the mix operators. This means that authentication of the user is required by the mix.

As already stated when the mix is processing messages for a user it has no knowledge of who the user is. Authenticating the user must therefore not reveal to the mix the users identification. One way to achieve this is for the mix to charge a flat rate to the user and perform authentication on a token basis. Tokens can be issued to the user via a blinding protocol. These protocols would allow the mix to issue tokens without knowledge of who they were issued to so that on receipt they could be validated but not linked to a user. Such protocols are found within electronic commerce to issue digital coins, an example of which is Chaum's work in [23].

5.2. Information Leaking

There may be instances where a trusted third party requires the private information concerning a user's identity and location, e.g. the company fleet application mentioned in section 3. Under such conditions the location and identification must become available through the network to these end users. This is quite simple to achieve on an end-to-end basis since the user can request from the local network (with whom it has already been authenticated and which is keeping track of the users location) it's current location and then transmit this with it's identity within a secure anonymous message to the requesting end user.

An alternative to this approach is to store the information at the users HLR in a way that it is then only readable by an authenticated end user. The problem here is in the key distribution. If the same key is used for

decryption at all times then it assumes an end user always has permission to the information. This may not be the case. If a session key is used then when should this key be replaced. It is unreasonable for the HLR to keep a copy of the location information for each user who wishes to know it so it must also be a shared key between any authenticated party. It is another goal of this research to provide a mechanism to enable authenticated parties to query the HLR for a users location information.

5.3 Billing Requirements

Billing users for services is required in mobile networks. The situation is complicated even further by the fact that foreign networks may have to bill the users home network when the user receives service within the foreign network. In conventional billing systems a specific user is charged for a specific service. In order to achieve the privacy requirements set out in this paper and yet satisfy the network requirements for billing, communications must be anonymous yet accountable. This presents an obvious problem in that linking communications to a user will form a track of that users activities. Clearly this is not appropriate according to the users privacy requirements.

A solution to this problem is to use an anonymous tokening system such as those found in electronic commerce. A users home network could provide tokens to the user which could be stored onto their subscriber identity module (SIM) and then used as the user receives service from the network. When the user runs out of tokens then the user can simply put more onto the card over the network by logging onto their account within the home network. As with normal billing, the number of token used would then indicate to the network how much to bill the user. Note that these tokens could even be electronic money, but for simplicity it is better to consider them as tokens only.

When the network issues the tokens they can be blinded by using techniques such as those outlined in Chaum [23]. The network will be able to check the validity of the token but not to whom it was issued. As these token will be used for billing the value of the token is recorded against the user account, prior to being issued blinded. When a part of a network attempts to redeem the token they can be validated on-line but, since the token value is already accredited to the user the origin of the token is not important to the home network. An invalid token will mean that the network refuses service. Note that according to these schemes, a user attempting to reuse a token will have their identity revealed.

6. Conclusion and Future Work

Modern mobile networks will allow users to roam into any location and still maintain a level of service at any time. A major concern is the privacy provided by the networks. In addition to providing content privacy users expect their location and identification information to be treated as confidential. Privacy from the networks as well as from third parties is required. In order to do so an element of trust is required. This is achieved through a user smart card (SIM) which holds secret keys enabling the user to set up secure communications with the network and with other users.

Mobile networks operate by holding routing information which is updated as the users move around. In order to do so in a secure manner the user should move around under a pseudonym. A user can do this by agreeing with their home location a pseudonym at registration. The connection between their identification, the pseudonym, and their location must be hidden from the parts of the network that hold these details individually.

Existing work in the field is examined and it is discussed that current approaches do not achieve an adequate level of protection of user information from the network. The proposed research in this paper would allow the requirements for user privacy to be achieved to an extent that has not been attained before.

Anonymity of communication can be provided by the use of a digital mix as proposed by Chaum in [20]. However operation of a mix in mobile networks where the users location is dynamic would render a traditional mix inefficient. Development of a mix that could cope with this kind of dynamic behaviour would be of benefit to network traffic whilst solving a difficult security problem. In addition it is proposed that these mixes should operate independently to the network with users paying for such a service. An implication of this is that mix-user authentication is required, a feature not required in other mix implementations.

Billing within mobile networks is a problem and being able to provide anonymous yet accountable service would be a novel step forwards. To achieve total privacy in this manner would be very important since it would allow users to gain a higher level of trust of foreign networks whilst allowing these networks to operate effectively.

An implementation of the proposed ideas in this paper has begun. This implementation will simulate the mobile network architecture and allow the development and testing of the new authentication, digital mix, information leaking, and billing services that are needed to provide the required user privacy.

References

- [1] J. C. Arnbak and J. M. G. Linnartz, "The European Recipe Mix for Mobile Networking: Technology, Policy and Markets," proc. IFIP/TC6 Personal Wireless Communications, Prague, 1995, pp. 1-19.
- [2] T. Magedanz, "Integration and Evolution of Existing Mobile Telecommunications Systems towards UMTS," IEEE Communications Magazine, vol. 29, no. 9, pp. 90-96, 1996.
- [3] M. Rahnema, "Overview of the GSM System and Protocol Architecture," *IEEE Communications Magazine*, vol. 26, no. 4, pp. 92-100, 1993.
- [4] S. S. Husain and J. A. Marocchi, "Intelligent Network: A Key Platform for PCS Interworking and Interoperability," *IEEE Communications Magazine*, vol. 29, no. 9, pp. 98-105, 1996.
- [5] I. F. Akyildiz and J. S. M. Ho, "On Location Management for Personal Communications Networks," *IEEE Communications Magazine*, vol. 29, no. 9, pp. 138-145, 1996.
- [6] C. P. Pfleeger, "Security In Computing," 1st ed: Prentice Hall International, 1989.
- [7] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
- [8] B. C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications Magazine*, vol. 27, no. 9, pp. 33-38, 1994.
- [9] H. Federrath, A. Jerichow, D. Kesdogan, and A. Pfitzman, "Security in Public Mobile Communication Networks," proc. IFIP/TC6 Personal Wireless Communications, Prague, 1995, pp. 105-116.
- [10] S. T. Walker, S. B. Lipner, C. M. Ellison and D. M. Balenson, "Commercial Key Recovery," Communications of the ACM, vol. 39, no. 3, -, 1996.
- [11] GSM Security, Internet Document: http://www.tele.pw.edu.pl/Pl-iso/~kwrona/gsm/gsm.html.
- [12] B. Pfitzmann, "Digital Signature Schemes: General Framework and Fail-Stop Signatures." Berlin: Springer-Verlag, 1996.

- [13] A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks," *IEEE Personal Communications*, vol. 1, no. 1, pp. 25-31, 1994.
- [14] R. Molva, D. Samfat, and G. Tsudik, "Authentication of Mobile Users," *IEEE Network*, vol. 8, no. 2, pp. 26-34, 1994.
- [15] M. J. Beller, L. Chang, and Y. Yacobi, "Privacy and Authentication on a Portable Communications System," *IEEE Selected Areas In Communications*, vol. 11, no.6, pp. 821-829, 1993.
- [16] U. Carlsen, "Optimal Privacy and Authentication on a Portable Communications System," Operating Systems Review, vol. 28, no.3, pp. 11-23, 1994.
- [17] V. Bharghavan, "Secure Wireless LANs," proc. ACM Computer and Communications Security, Fairfax, Virginia, 1994, pp. 10-17.
- [18] S. Hoff, K. Jakobs, and D. Kesdogan, "Anonymous Mobility Management for Third Generation Mobile Networks," proc. IFIP/TC6&TC11 Communications and Multimedia Security, Essen, Germany, 1996, pp. 72-83.
- [19] D. A. Cooper and K. P. Birman, "Preserving Privacy in a Network of Mobile Computers," proc. IEEE Symposium on Research in Security and Privacy, Oakland, California, 1995, pp. 26-38.
- [20] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84-88, 1981.
- [21] C. Gulcu and G. Tsudik, "Mixing E-mail with BABEL." proc. Symposium on Networks and Distributed Systems Security, -, 1996, pp. 2-16.
- [22] C. H. Fancher, "In Your Pocket Smartcards," IEEE Spectrum, vol. 34, no. 2, pp. 47-53, 1997.
- [23] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030-1044, 1985.

```
Description
Set
        Items
                S COMPUTER? ? OR CPU? ? OR CENTRAL() PROCESSING OR PROCESSOR? ? OR SERVER?
S1
      7449240
? OR MINICOMPUTER? ? OR MICROCOMPUTER? ? OR PC OR LAPTOP? ? OR HANDHELD? ? OR NOTEBOOK? ?
OR COMPUTING OR MAINFRAME? ? OR MAIN()(FRAME OR FRAMES) OR SYSTEM? ? OR SELF()SERVIC? OR
ATM OR ATMS OR ((AUTOMATED OR AUTOMATIC)()(TELLER OR TRANSACTION OR SERVICE) OR CASH OR
MONEY OR BANK) (W) (MACHINE? OR TERMINAL? ?) OR ELECTRONIC() TELLER? ?
                S VIRTUAL OR ONLINE OR ON()LINE OR INTERNET OR NET OR WEB OR WWW OR CYBER
     11018070
OR ELECTRONIC OR WEBSITE? OR WEBPAGE? OR WEB()(SITE? OR SERVER? ?)
                ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNSPECIF? OR
      1304000
UNKNOWN OR ?NO? (2N) (PERSONAL OR USER) FROM 20
                S S3(5N)(DATA OR DEMOGRAPHIC? ? OR INFORMATION OR NUMBER? ? OR
IDENTIFICATION OR NAME? ? OR ID)
                S PASSWORD OR PIN OR PERSONAL()(IDENTIFICATION OR ID)()NUMBER OR CODE OR
      3656430
KEY OR (PASS OR SECRET)()(WORD? ? OR PHRASE? ? OR NUMBER? ?) OR PASSPHRASE OR PASSNUMBER
OR (SECURITY OR ACCESS)()(CODE? ? OR KEY? ?) OR USER()(ID OR IDENTIFICATION OR NAME)
                S LOGON OR LOGIN OR (LOG OR LOGG? OR SIGN OR SIGNING OR SIGNED) () (IN OR
ON) OR AUTHENTICAT? OR (UNIQUE OR UNCOMMON OR DISTINGUISHING OR
DISTINCTIVE) (10N) (INFORMATION OR DATA OR STATISTIC? ? OR NUMBER? ?)
                S PATRON? ? OR CUSTOMER? ? OR CLIENT? ? OR USER? ? OR SUBSCRIBER? ? OR
ENROLEE? ? OR PARTICIPANT? ? OR PARTICIPAT?R? ? OR PERSON? ? OR DRIVER? ? OR OPERATOR? ?
(5N) GENERAT??? OR ACCOMPLISH? OR BRING() ABOUT OR CREATE? OR FORM? ? OR INITIAT?
                S TRANSACTION? ? OR ORDER? ? OR PROCEDURE? ? OR INTERACTION? ? OR DEALING?
     22039075
? OR ACTION? ? OR TRADE? ? OR TRADING OR PURCHAS??? OR EXCHANG??? OR DEAL? ? OR SELL??? OR
SALE? ? OR BUY???
                S S1(S)S4
         5481
                S S2(S)S4
         8633
S10
                S S7(S)S5
       856242
S11
                S S7(S)S6
       130415
S12
                S S7(S)(S5 AND S6).
S13
        68248
                S (S1 OR S2)(S)S4
        12037
S14
                S S13(S)S14
          212
S15
                S S15(S)S8
           89
S16
                S S16 NOT PY>1998
S17
            6
                     (unique items)
S18
            6
                'RD
 ; show files
```

[File 20] Dialog Global Reporter 1997-2007/Feb 06

(c) 2007 Dialog. All rights reserved.

18/3,K/1 Links

Dialog Global Reporter

(c) 2007 Dialog. All rights reserved.

03461465 (USE FORMAT 7 OR 9 FOR FULLTEXT)

EXCITE: This season it's a wonderful excite

M2 PRESSWIRE

November 16, 1998

Journal Code: WMPR Language: English Record Type: FULLTEXT

Word Count: 722

(USE FORMAT 7 OR 9 FOR FULLTEXT)

...information. Just register once by filling-out the one-page Express Order form, choose a **secret user name** and **password** and that's it. Crossing everyone off that every growing qift list is just a...

18/3,K/2 Links

Dialog Global Reporter

(c) 2007 Dialog. All rights reserved.

03452855 (USE FORMAT 7 OR 9 FOR FULLTEXT)

This Season It's a Wonderful Excite: Jingle Bells, Mistletoe and Virtual Elves To the Rescue

PR NEWSWIRE

November 16, 1998

Journal Code: WPRW Language: English Record Type: FULLTEXT

Word Count: 715

(USE FORMAT 7 OR 9 FOR FULLTEXT)

...information. Just register once by filling-out the one-page Express Order form, choose a **secret user name** and **password** and that's it. Crossing everyone off that every growing gift list is just a...

18/3,K/3 Links

Dialog Global Reporter

(c) 2007 Dialog. All rights reserved.

02903187

e-Net, Inc. Introduces TelSet Express(TM) - Software Solution Enabling Customers of Participating Data Service Providers to Tap Benefits of Data Telephony(TM) & Use Advanced Calling Features

PR NEWSWIRE

September 23, 1998

Journal Code: WPRW Language: English Record Type: FULLTEXT

Word Count: 815

...expressions are intended to identify forward-looking statements. These forward-looking statements involve known and unknown risks and uncertainties. For additional information regarding these and other risks and uncertainties associated with the Company's business, reference is made to the Company's reports filed from time to time with the Securities and Exchange Commission. For more information on Telecom 2000a or other e-Net products, visit the company's Web site at http://www.datatelephony.com, call e-Net at 1-888-FON- ENET or 301-601-8700, or fax e-Net at 301-601-8777. /CONTACT: Media, Paul D. Feldman, 410-571-8900, FelCom@AOL.com or www.FeldmanCommunications.com; or investor, Doug Poretz, 703-506-1778, ext. 222, doug@poretz.com or www.poretz.com, both for e-Net/ 11:38 EDT

18/3,K/4 Links

Dialog Global Reporter
(c) 2007 Dialog. All rights reserved.
02414948 (USE FORMAT 7 OR 9 FOR FULLTEXT)
File Business and Trade References On Line

BUSINESS WIRE

August 04, 1998 12:44

Journal Code: WBWE Language: English Record Type: FULLTEXT

Word Count: 283

(USE FORMAT 7 OR 9 FOR FULLTEXT)

...they can use to provide credit and trade information about the program participant -- discreetly and **on line. www**.isitsafe.com is a secure site, and every three months references are reminded by email...

18/3,K/5 <u>Links</u>

Dialog Global Reporter

(c) 2007 Dialog. All rights reserved.

01773634

Penn State to Introduce On-Line, ID Card Systems

Tom Gibb

KRTBN KNIGHT-RIDDER TRIBUNE BUSINESS NEWS (PITTSBURGH POST-GAZETTE)

May 28, 1998 21:7

Journal Code: KPPG Language: English Record Type: FULLTEXT

Word Count: 749

...cards when they have added value." Penn State could use the card to track student **buying** habits -- or evento see who in the student body hasn't done a stitch of...

...attending any PennState campus to plot their academic life on-line.
"There's virtually no **system** like this in the United States," Penn
StatePresident Graham Spanier said. "There are companies charging millions ofdollars to come up with **systems** that do only part of what this one does." Since the fall, the **system** has let students sign on at any time andcheck grades, calculate the credits they need...

...status of student loansand getting them in or out of courses. It's also an **electronic** link that allows messages to be **traded** betweenacademic advisers and advisees. "It's been suggested that students just be allowed to enter...

...that it does what it used to take letters, phone calls and office visits to accomplish. Another advantage is that the system is open all hours. "Students suddenly remember they need this information at 11 o'clock...

...university coordinator for certification and educationservices. More than 600 students have been tapping into the **system** daily. But theycan't get to their own records without using personal **security** codes, Wagersaid. Grow, also an adviser in the College of Education, insisted CAAISdoesn't build distance...

...yet I was closer to himthan to other advisees," Grow said. Students without access to **computers** can still register for courses theold fashioned way, by phone, and get the same shot...

18/3,K/6 Links .

Dialog Global Reporter

(c) 2007 Dialog. All rights reserved.

01269382 (USE FORMAT 7 OR 9 FOR FULLTEXT)

'On Your Mouse, Get 'Net, Go!': The 'New and Improved' MCI Great American Net Test to Measure Nation's Internet Aptitude

BUSINESS WIRE

March 30, 1998 8:4

Journal Code: WBWE Language: English Record Type: FULLTEXT

Word Count: 1000

...compared to determine if the country's Internet skills are improving. "Americans are encouraged to **log on** to this year's test to be

counted," added Price, in this annual benchmarking competition. The site (www.nettest.mci.com) will be on-line through July 4, 1998. Are America's Internet skills improving?

```
Set Items Description
   5056344 S COMPUTER? ? OR CPU? ? OR CENTRAL()PROCESSING OR PROCESSOR? ? OR SERVER? ? OR
MINICOMPUTER?? OR MICROCOMPUTER?? OR PC OR LAPTOP?? OR HANDHELD?? OR NOTEBOOK?? OR
COMPUTING OR MAINFRAME? ? OR MAIN()(FRAME OR FRAMES) OR SYSTEM? ? OR SELF()SERVIC? OR ATM OR
ATMS OR ((AUTOMATED OR AUTOMATIC)()(TELLER OR TRANSACTION OR SERVICE) OR CASH OR MONEY OR
BANK) (W)(MACHINE? OR TERMINAL? ?) OR ELECTRONIC()TELLER? ?
S2 5950852 S VIRTUAL OR ONLINE OR ON()LINE OR INTERNET OR NET OR WEB OR WWW OR CYBER OR
ELECTRONIC OR WEBSITE? OR WEBPAGE? OR WEB()(SITE? OR SERVER? ?)
   471870 ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNSPECIF? OR
UNKNOWN OR ?NO?(2N)(PERSONAL OR USER) FROM 15, 610, 810, 476, 613, 813, 634, 624
     31027 S S3(5N)(DATA OR DEMOGRAPHIC?? OR INFORMATION OR NUMBER?? OR IDENTIFICATION OR
NAME? ? OR ID)
S5 2129390 S PASSWORD OR PIN OR PERSONAL()(IDENTIFICATION OR ID)()NUMBER OR CODE OR KEY OR
(PASS OR SECRET)()(WORD? ? OR PHRASE? ? OR NUMBER? ?) OR PASSPHRASE OR PASSNUMBER OR
(SECURITY OR ACCESS)()(CODE?? OR KEY??) OR USER()(ID OR IDENTIFICATION OR NAME)
    468778 S LOGON OR LOGIN OR (LOG OR LOGG? OR SIGN OR SIGNING OR SIGNED)()(IN OR ON) OR
AUTHENTICAT? OR (UNIQUE OR UNCOMMON OR DISTINGUISHING OR DISTINCTIVE)(10N)(INFORMATION OR
DATA OR STATISTIC? ? OR NUMBER? ?)
S7 6501915 S PATRON? ? OR CUSTOMER? ? OR CLIENT? ? OR USER? ? OR SUBSCRIBER? ? OR ENROLEE? ?
OR PARTICIPANT?? OR PARTICIPAT?R?? OR PERSON?? OR DRIVER?? OR OPERATOR?? (5N) GENERAT???
OR ACCOMPLISH? OR BRING()ABOUT OR CREATE? OR FORM?? OR INITIAT?
S8 8438653 S TRANSACTION?? OR ORDER?? OR PROCEDURE?? OR INTERACTION?? OR DEALING?? OR
ACTION? ? OR TRADE? ? OR TRADING OR PURCHAS??? OR EXCHANG??? OR DEAL? ? OR SELL??? OR SALE? ?
OR BUY???
     4123 S S1(S)S4
S9
     5054 S S2(S)S4
S10
     661051 S S7(S)S5
S11
    112365 S S7(S)S6
S12
     86402 S S7(S)(S5 AND S6)
S13
      7753 S (S1 OR S2)(S)S4
S14
      267 S S13(S)S14
S15
      94 S S15(S)S8
S16
S17
      2352 S S4(S)(S5 OR S6)
      1261 S S17(S)S7
S18
      639 S S18(S)(S1 OR S2)
S19
      452 S S18(S)S1
S20
      404 S S18(S)S2
S21
      143 S S20(S)S8
$22
      150 S S21(S)S8
S23
      1135 S S4(10N)(S5 OR S6)
S24
      464 S S24(20N)S7
S25
S26
      324 S S24(5N)S7
      812 S S4(5N)S5
S27
      204 S S4(5N)S6
S28
      959 S S27 OR S28
S29
       57 S S27 AND S28
S30
       31 S S30(10N)S7
S31
S32
       22 S S31 NOT PY>1998
 ; show files
```

[File 15] ABI/Inform(R) 1971-2007/Feb 03

(c) 2007 ProQuest Info&Learning. All rights reserved.

[File 610] Business Wire 1999-2007/Feb 06 (c) 2007 Business Wire. All rights reserved.

*File 610: File 610 now contains data from 3/99 forward. Archive data (1986-2/99) is available in File 810.

[File 810] Business Wire 1986-1999/Feb 28

(c) 1999 Business Wire . All rights reserved.

[File 476] Financial Times Fulltext 1982-2007/Feb 06

(c) 2007 Financial Times Ltd. All rights reserved.

[File 613] PR Newswire 1999-2007/Feb 06

(c) 2007 PR Newswire Association Inc. All rights reserved.

*File 613: File 613 now contains data from 5/99 forward. Archive data (1987-4/99) is available in File 813.

[File 813] PR Newswire 1987-1999/Apr 30

(c) 1999 PR Newswire Association Inc. All rights reserved.

[File 634] San Jose Mercury Jun 1985-2007/Feb 02

(c) 2007 San Jose Mercury News. All rights reserved.

[File 624] McGraw-Hill Publications 1985-2007/Feb 06

(c) 2007 McGraw-Hill Co. Inc. All rights reserved.

*File 624: Homeland Security & Defense and 9 Platt energy journals added Please see HELP NEWS624 for more

32/3,K/3 (Item 3 from file: 15) Links

ABI/Inform(R)

(c) 2007 ProQuest Info&Learning. All rights reserved.

01421888

00-72875

Keep out prying eyes

Elledge, Don

Informationweek n629 pp: 102-110

May 5, 1997

ISSN: 8750-6874 Journal Code: IWK

Word Count: 3113

Text:

...registry to store IDs and passwords for all entities, it solves the problem of multiple ID and password pairs.

Secret keys for authentication between entities are distributed on an as-needed basis. Users log on once, and then can access all resources within the environment to which they...

32/3,K/5 (Item 5 from file: 15) Links

ABI/Inform(R)

(c) 2007 ProQuest Info&Learning. All rights reserved.

01222439

98-71834

How to keep someone from hiding in plain view

Schwartau, Winn

Network World v13n22 pp: 39-40

May 27, 1996

ISSN: 0887-7661 Journal Code: NWW

Word Count: 1139

Text:

...as all people with an address ending in .edu, or do you enforce a stronger user-identification and authentication mechanism?

Remotely anonymous

Dial-up ports into organizations present similar opportunities to the bad guys. Once your password...

32/3,K/14 (Item 3 from file: 810) Links

Business Wire

(c) 1999 Business Wire . All rights reserved.

0731671 BW1171

SECURITY DYNAMICS : Security Dynamics Enhances Solution for Secure Remote Access

August 05, 1997

Byline: Business/Technology Editors

...authentication software generates a new access code every 60 seconds that, when combined with the user's secret personal identification number (PIN), authenticates the user attempting to access a protected network. SoftID authentication software works in conjunction with Security Dynamics...

t s32/6/all

32/6/1 (Item 1 from file: 15) Links

02320273

86925987

USE FORMAT 7 OR 9 FOR FULL TEXT

The UNIverse Project: state-of-the-art of the standards, softwares and systems which will underpin the development. Part 3: inter library loans protocols multimedia document delivery and authentication and directory services

1998

Word Count: 5493

32/6/2 (Item 2 from file: 15) Links

01691972

03-42962

USE FORMAT 7 OR 9 FOR FULL TEXT

The keys to security

Aug 31, 1998 Length: 5 Pages

Word Count: 1731

32/6/3 (Item 3 from file: 15) **Links**

01421888

00-72875

USE FORMAT 7 OR 9 FOR FULL TEXT

Keep out prying eyes

May 5, 1997 Length: 6 Pages

Word Count: 3113

32/6/4 (Item 4 from file: 15) Links

01403841

00054828

USE FORMAT 7 OR 9 FOR FULL TEXT

Web sites that shine

Feb 24, 1997 Length: 5 Pages

Word Count: 2756

32/6/5 (Item 5 from file: 15) Links

01222439

98-71834

USE FORMAT 7 OR 9 FOR FULL TEXT

How to keep someone from hiding in plain view

May 27, 1996 Length: 2 Pages

Word Count: 1139

32/6/6 (Item 6 from file: 15) Links

01023329

96-72722

USE FORMAT 7 OR 9 FOR FULL TEXT

Financial services can now be offered on Internet

May 1995 Length: 1 Pages

Word Count: 850

32/6/7 (Item 7 from file: 15) Links

00930359

95-79751

USE FORMAT 7 OR 9 FOR FULL TEXT

Smart cards: The next generation

Sep 1994 Length: 3 Pages

Word Count: 1639

32/6/8 (Item 8 from file: 15) Links

00880405

95-29797

USE FORMAT 7 OR 9 FOR FULL TEXT

Using Fetch, the wonder retriever for FTP

Jul 1994 Length: 4 Pages

Word Count: 1102

32/6/9 (Item 9 from file: 15) Links

00860584

95-09976

USE FORMAT 7 OR 9 FOR FULL TEXT

The danger in FTP

May 16, 1994 Length: 1 Pages

Word Count: 377

32/6/10 (Item 10 from file: 15) Links

00860581

95-09973

USE FORMAT 7 OR 9 FOR FULL TEXT

Repelling the wily hacker

May 16, 1994 Length: 3 Pages

Word Count: 2361

32/6/11 (Item 11 from file: 15) Links

00481175

90-06932

Plan for Nitty Gritty in UNIX Changeover (Part 6)

Dec 1989 Length: 1 Pages

32/6/12 (Item 1 from file: 810) Links

0951691 BW1385

OCG TECHNOLOGIES: Internet Service introduced by OCG Technology

December 14, 1998

32/6/13 (Item 2 from file: 810) Links

0950973 BW1200

OCG TECHNOLOGIES : Internet Service introduced by OCG Technology

December 11, 1998

32/6/14 (Item 3 from file: 810) Links

0731671 BW1171

SECURITY DYNAMICS: Security Dynamics Enhances Solution for Secure Remote Access

August 05, 1997

32/6/15 (Item 4 from file: 810) Links

0711169 BW1138

AXENT 2: AXENT's OmniGuard/ESM 4.4 identifies more than 90 security weaknesses in Windows NT

June 09, 1997

32/6/16 (Item 5 from file: 810) Links

0675005 BW0089

PEP INC: New PC smart card reader boosts online transaction security; Southern California firm introduces "Authenticator" to eliminate transaction interception, hacker decoding, fraud risk

February 24, 1997

32/6/17 (Item 6 from file: 810) Links

0432750 BW1094

COMPAQ COMPUTER: Compaq Announces Customer Support On The Internet

September 28, 1994

32/6/18 (Item 7 from file: 810) Links

0262367 BW693

SECURITY DYNAMICS: Security Dynamics granted temporary restraining order against TymTech

January 29, 1992

32/6/19 (Item 1 from file: 813) Links

0855726

AT014

SCIENTIFIC-ATLANTA TO PROVIDE GROUND STATIONS TO E-SYSTEMS FOR SPACE IMAGING INC.

Date: August 31, 1995 Word Count: 511

32/6/20 (Item 2 from file: 813) Links

0740473

DC035

GSA DOD RELEASE FINAL ELECTRONIC COMMERCE ACQUISITION GUIDELINES; GSA'S JOHNSON SAYS GUIDELINES WILL REFORM FEDERAL PROCUREMENT AND PRODUCE EFFICIENCY AND SAVINGS

Date: September 9, 1994

Word Count: 780

32/6/21 (Item 1 from file: 624) **Links**

0643289

WARDING OFF THE CYBERSPACE INVADERS: Internet crime is rising, but there are ways to reduce the threat

March 13, 1995

WORD COUNT: 1,239

32/6/22 (Item 2 from file: 624) <u>Links</u>

0495714 Locating and Retrieving Internet Files July, 1993 WORD COUNT: 2,153

Set Items Description S1 15702375 S COMPUTER? ? OR CPU? ? OR CENTRAL()PROCESSING OR PROCESSOR? ? OR SERVER? ? OR MINICOMPUTER?? OR MICROCOMPUTER?? OR PC OR LAPTOP?? OR HANDHELD?? OR NOTEBOOK?? OR COMPUTING OR MAINFRAME? ? OR MAIN()(FRAME OR FRAMES) OR SYSTEM? ? OR SELF()SERVIC? OR ATM OR ATMS OR ((AUTOMATED OR AUTOMATIC)()(TELLER OR TRANSACTION OR SERVICE) OR CASH OR MONEY OR BANK) (W)(MACHINE? OR TERMINAL? ?) OR ELECTRONIC()TELLER? ? S2 17221272 S VIRTUAL OR ONLINE OR ON()LINE OR INTERNET OR NET OR WEB OR WWW OR CYBER OR ELECTRONIC OR WEBSITE? OR WEBPAGE? OR WEB()(SITE? OR SERVER??) S3 1171702 ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNSPECIF? OR UNKNOWN OR ?NO?(2N)(PERSONAL OR USER) FROM 9, 275, 621, 636, 16, 160, 148 80752 S S3(5N)(DATA OR DEMOGRAPHIC? ? OR INFORMATION OR NUMBER? ? OR IDENTIFICATION OR NAME? ? OR ID) S5 5338001 S PASSWORD OR PIN OR PERSONAL()(IDENTIFICATION OR ID)()NUMBER OR CODE OR KEY OR (PASS OR SECRET)()(WORD?? OR PHRASE?? OR NUMBER??) OR PASSPHRASE OR PASSNUMBER OR (SECURITY OR ACCESS)()(CODE? ? OR KEY? ?) OR USER()(ID OR IDENTIFICATION OR NAME) 842908 S LOGON OR LOGIN OR (LOG OR LOGG? OR SIGN OR SIGNING OR SIGNED)()(IN OR ON) OR AUTHENTICAT? OR (UNIQUE OR UNCOMMON OR DISTINGUISHING OR DISTINCTIVE)(10N)(INFORMATION OR DATA OR STATISTIC? ? OR NUMBER? ?) 462804 S (PATRON? ? OR CUSTOMER? ? OR CLIENT? ? R PERSON? ? OR DRIVER? ? OR OPERATOR? ?)(5N)(GENERAT??? OR ACCOMPLISH? OR BRING()ABOUT OR CREATE? OR FORM? ? OR INITIAT?) 2394236 S TRANSACTION?? S9 2827 S S4(10N)S5 S10 859 S S4(10N)S6 337 S S9 AND S10 S11 0 S S11(10N)S7 S12 0 S S11(S)S7 S13 5534 S S4(S)S5 S14 1572 S S4(S)S6 S15 702 S S14 AND S15 S16 9 S S16(S)S7 S17 1 S S17 NOT PY>1998 S18 ; show files [File 9] Business & Industry(R) Jul/1994-2007/Feb 05 (c) 2007 The Gale Group. All rights reserved. [File 275] Gale Group Computer DB(TM) 1983-2007/Feb 02

(c) 2007 The Gale Group. All rights reserved.

[File 621] Gale Group New Prod.Annou.(R) 1985-2007/Jan 29

(c) 2007 The Gale Group. All rights reserved.

[File 636] Gale Group Newsletter DB(TM) 1987-2007/Feb 02

(c) 2007 The Gale Group. All rights reserved.

[File 16] Gale Group PROMT(R) 1990-2007/Feb 02

(c) 2007 The Gale Group. All rights reserved.

[File 160] Gale Group PROMT(R) 1972-1989

(c) 1999 The Gale Group. All rights reserved.

[File 148] Gale Group Trade & Industry DB 1976-2007/Jan 29

(c)2007 The Gale Group. All rights reserved.

18/3,K/1 (Item 1 from file: 636) Links

Gale Group Newsletter DB(TM)

(c) 2007 The Gale Group. All rights reserved.

03667021 Supplier Number: 47899724 (USE FORMAT 7 FOR FULLTEXT)

SECURITY DYNAMICS: Security Dynamics launches new version of SoftID authentication software

M2 Presswire, p N/A

August 11, 1997

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 616

...to install and use, but still allowing remote network access.

The new version of SoftID **authentication** software allows installation to take place over the network. Previously, installation could only be accomplished...

...access from a shared machine can be accomplished without end users having to share their **secret** PINs. Customisable **information** fields have been added to the SoftID administration program to allow tracking of additional user...

... The administration program also allows user information to be edited after a SoftID has been **created**.

"Time and time again our **customers** tell us that one of their top requirements for security products is making them easier...

```
Description
Set
        Items
                S COMPUTER? ? OR CPU? ? OR CENTRAL()PROCESSING OR PROCESSOR? ? OR SERVER?
        29321
Sl
? OR MINICOMPUTER? ? OR MICROCOMPUTER? ? OR PC OR LAPTOP? ? OR HANDHELD? ? OR NOTEBOOK? ?
OR COMPUTING OR MAINFRAME? ? OR MAIN()(FRAME OR FRAMES) OR SYSTEM? ? OR SELF()SERVIC? OR
ATM OR ATMS OR ((AUTOMATED OR AUTOMATIC)()(TELLER OR TRANSACTION OR SERVICE) OR CASH OR
MONEY OR BANK) (W) (MACHINE? OR TERMINAL? ?) OR ELECTRONIC() TELLER? ?
               S VIRTUAL OR ONLINE OR ON()LINE OR INTERNET OR NET OR WEB OR WWW OR CYBER
        19027
OR ELECTRONIC OR WEBSITE? OR WEBPAGE? OR WEB()(SITE? OR SERVER? ?)
               ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNSPECIF? OR
UNKNOWN OR ?NO? (2N) (PERSONAL OR USER) FROM 256
               S S3(5N)(DATA OR DEMOGRAPHIC? ? OR INFORMATION OR NUMBER? ? OR
IDENTIFICATION OR NAME? ? OR ID)
                S PASSWORD OR PIN OR PERSONAL()(IDENTIFICATION OR ID)()NUMBER OR CODE OR
KEY OR (PASS OR SECRET)()(WORD? ? OR PHRASE? ? OR NUMBER? ?) OR PASSPHRASE OR PASSNUMBER
OR (SECURITY OR ACCESS)()(CODE? ? OR KEY? ?) OR USER()(ID OR IDENTIFICATION OR NAME)
                S LOGON OR LOGIN OR (LOG OR LOGG? OR SIGN OR SIGNING OR SIGNED) () (IN OR
ON) OR AUTHENTICAT? OR (UNIQUE OR UNCOMMON OR DISTINGUISHING OR
DISTINCTIVE) (10N) (INFORMATION OR DATA OR STATISTIC? ? OR NUMBER? ?)
        21752 S PATRON? ? OR CUSTOMER? ? OR CLIENT? ? OR USER? ? OR SUBSCRIBER? ? OR
ENROLEE? ? OR PARTICIPANT? ? OR PARTICIPAT?R? ? OR PERSON? ? OR DRIVER? ? OR OPERATOR? ?
(5N) GENERAT??? OR ACCOMPLISH? OR BRING() ABOUT OR CREATE? OR FORM? ? OR INITIAT?
               S TRANSACTION? ? OR ORDER? ? OR PROCEDURE? ? OR INTERACTION? ? OR DEALING?
? OR ACTION? ? OR TRADE? ? OR TRADING OR PURCHAS??? OR EXCHANG??? OR DEAL? ? OR SELL??? OR
SALE? ? OR BUY???
               S S1(S)S4
           52
S9
                S S2(S)S4
           34
S10
         2793
               S S7(S)S5
S11
               S S7(S)S6
          963
S12
          277
              S S7(S)(S5 AND S6)
S13
           60
                S (S1 OR S2)(S)S4
S14
           60
                S (S1 OR S2)(S)S4
S15
                S. S4(S)S5
           15
S16
           7
                S S4(S)S6
S17
                S S16 AND S17
S18
            0
                S S18 NOT PY>1998
S19
```

[File 256] TecInfoSource 82-2007/Aug

; show files

(c) 2007 Info. Sources Inc. All rights reserved.

Set Items Description

S1 1008474 S COMPUTER?? OR CPU?? OR CENTRAL()PROCESSING OR PROCESSOR?? OR SERVER?? OR MINICOMPUTER?? OR MICROCOMPUTER?? OR PC OR LAPTOP?? OR HANDHELD?? OR NOTEBOOK?? OR COMPUTING OR MAINFRAME?? OR MAIN()(FRAME OR FRAMES) OR SYSTEM?? OR SELF()SERVIC? OR ATM OR ATMS OR ((AUTOMATED OR AUTOMATIC)()(TELLER OR TRANSACTION OR SERVICE) OR CASH OR MONEY OR BANK) (W)(MACHINE? OR TERMINAL??) OR ELECTRONIC()TELLER??

S2 1944410 S VIRTUAL OR ONLINE OR ON()LINE OR INTERNET OR NET OR WEB OR WWW OR CYBER OR ELECTRONIC OR WEBSITE? OR WEBPAGE? OR WEB()(SITE? OR SERVER? ?)

- S3 143571 ANONYM? OR INCOG? OR PSEUDO? OR SECRET OR UNDISCLOSE? OR UNSPECIF? OR UNKNOWN OR ?NO?(2N)(PERSONAL OR USER) FROM 625, 268, 626, 267, 608
- 9083 S S3(5N)(DATA OR DEMOGRAPHIC? ? OR INFORMATION OR NUMBER? ? OR IDENTIFICATION OR NAME? ? OR ID)
- S5 400815 S PASSWORD OR PIN OR PERSONAL()(IDENTIFICATION OR ID)()NUMBER OR CODE OR KEY OR (PASS OR SECRET)()(WORD?? OR PHRASE?? OR NUMBER??) OR PASSPHRASE OR PASSNUMBER OR (SECURITY OR ACCESS)()(CODE?? OR KEY??) OR USER()(ID OR IDENTIFICATION OR NAME)
- S6 55528 S LOGON OR LOGIN OR (LOG OR LOGG? OR SIGN OR SIGNING OR SIGNED)()(IN OR ON) OR AUTHENTICAT? OR (UNIQUE OR UNCOMMON OR DISTINGUISHING OR DISTINCTIVE)(10N)(INFORMATION OR DATA OR STATISTIC? ? OR NUMBER? ?)
- S7 1639126 S PATRON?? OR CUSTOMER?? OR CLIENT?? OR USER?? OR SUBSCRIBER?? OR ENROLEE?? OR PARTICIPANT?? OR PARTICIPAT?R?? OR PERSON?? OR DRIVER?? OR OPERATOR?? (5N) GENERAT??? OR ACCOMPLISH? OR BRING()ABOUT OR CREATE? OR FORM?? OR INITIAT?
- S8 2436108 S TRANSACTION?? OR ORDER?? OR PROCEDURE?? OR INTERACTION?? OR DEALING?? OR ACTION?? OR TRADE?? OR TRADING OR PURCHAS??? OR EXCHANG??? OR DEAL?? OR SELL??? OR SALE?? OR BUY???
- S9 1459 S S1(S)S4
- S10 1616 S S2(S)S4
- S11 98388 S S7(S)S5
- S12 17180 S S7(S)S6
- S13 6622 S S7(S)(S5 AND S6)
- S14 2415 S (S1 OR S2)(S)S4
- S15 2415 S (S1 OR S2)(S)S4
- S16 673 S S4(S)S5
- S17 129 S S4(S)S6
- S18 53 S S16 AND S17
- S19 12 S S18 NOT PY>1998
- S20 12 RD (unique items)

; show files

[File 625] American Banker Publications 1981-2007/Feb 05

(c) 2007 American Banker. All rights reserved.

[File 268] Banking Info Source 1981-2007/Jan W4

(c) 2007 ProQuest Info&Learning. All rights reserved.

[File 626] Bond Buyer Full Text 1981-2007/Feb 06

(c) 2007 Bond Buyer. All rights reserved.

[File 267] Finance & Banking Newsletters 2007/Feb 05

(c) 2007 Dialog. All rights reserved.

[File 608] KR/T Bus.News. 1992-2007/Feb 06

(c)2007 Knight Ridder/Tribune Bus News. All rights reserved.

20/3,K/1 (Item 1 from file: 625) Links

American Banker Publications

(c) 2007 American Banker. All rights reserved.

0195280

Card Frontiers: Gemplus in Deal with Maker of Random-Password Device; Many Uses Seen

American Banker - February 26, 1997; Pg. 12; Vol. 162, No. 38 Document Type: Journal Language: English Record Type: Fulltext

Word Count: 327

Byline:

By JEFFREY KUTLER

Text:

...has helped establish Security Dynamics as the world leader in what it calls two-factor authentication, with 1.5

million users in 1,600 companies. By combining a computer operator's secret

code with the random number, SecurID gets around one of the biggest

security hazards in on-line networks-the reusable password, which is especially vulnerable to hacker attacks.

Security Dynamics also gained the preeminent position in...

20/3,K/2 (Item 2 from file: 625) **Links**

American Banker Publications

(c) 2007 American Banker. All rights reserved.

0051045

Card-Size Device May Solve On-Line Password Security Problem

American Banker - April 9, 1986; Pg. 11; Vol. 151, No. 70

Word Count: 707

Byline:

By MICHAEL WEINSTEIN

Text:

...computer to verify the user's identity.

"It raises the level of security above a password," Mr. Darwin said. Now,

users generally enter a **secret password** - often issued by the **data** base

operator - to identify themselves when **logging on** to a computer system.

But computer security experts have never been entirely comfortable with the...

20/3,K/3 (Item 1 from file: 268) Links

Banking Info Source

(c) 2007 ProQuest Info&Learning. All rights reserved.

00349329 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Smart cards, coming up to bat

Bielski, Lauren

ABA Banking Journal, v 90, n 11, p 57-62, Nov 1998 Document Type: Journal Article Language: English

Record Type: Abstract Fulltext

Word Count: 01927

Abstract:

...standards will prompt many vendors, merchants, and ultimately consumers to begin using smart cards. The **key** is to develop multi-use smart cards. Some envision a future where the typical consumer would carry one card that houses **personal information**, **another** for business **authentication**, and another for cash replacement. A pilot launched in July 1998 with MBNA involves the...

20/3,K/4 (Item 2 from file: 268) Links

Banking Info Source

(c) 2007 ProQuest Info&Learning. All rights reserved.

00337584 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Smart cards

Anonymous

Retail Delivery Strategies, v 9, p 5-27, 1998 Document Type: Journal Article Article Type: News Language:

English Record Type: Abstract Fulltext

Word Count: 12720

...some basic knowledge and a little time, it is quite easy to read the machine **code** that software comprises. Most of the security features embedded into computer games can be cracked...

...owned by BULL S.A.) and no secret stored in the memory ever leaves this unique secure component inside the chip. Data residing in the host or terminal are sent to the card. This information is then combined with the information in the card and the secret keys in the chip are applied to algorithms. During this process, no secret ever leaves

...then sent back to the host or terminal. No indication of the value of the **key** the smart card has used is given to the outside world.

Using very sophisticated techniques...

20/3,K/5 (Item 3 from file: 268) **Links**

Banking Info Source

(c) 2007 ProQuest Info&Learning. All rights reserved.

00286194 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Is this network secure?

Noe, Jeffrey

America's Community Banker, v 5, n 5, p 12-16, May 1996 Document Type: Journal Article Language:

English Record Type: Abstract Fulltext

Word Count: 02541

...on as a unit by a computer.

DES enciphers and chains eight-byte blocks of data using a secret key to provide a unique result. The key is eight bytes long. Fifty-six of the key's bits are used in a mathematical permutation encrypting the data.

DES also generates a...

...that an unknown party can prove his or her identity by encrypting and returning a **pseudorandom number**—a random **number** generated by a definite, nonrandom computational process-sent from the controlling party using a secret **password** presumed to be known by both parties.

The controlling party then decrypts the result using...

20/3,K/6 (Item 4 from file: 268) Links

Banking Info Source

(c) 2007 ProQuest Info&Learning. All rights reserved.

00262267 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Financial services can now be offered on Internet

Anonymous

Bank Marketing, v 27, n 5, p.82, May 1995 Document Type: Journal Article Language: English Record

Type: Abstract Fulltext Word Count: 00850

...Web servers, Open Market claims its products handle the multi-dimensional issue of security. User **authentication** in the form of passwords, **secret numbers** and even smart cards can be implemented, as well as "smart statements" that pinpoint exact...

20/3.K/7 (Item 5 from file: 268) Links

Banking Info Source

(c) 2007 ProQuest Info&Learning. All rights reserved. 00242783 (USE FORMAT 7 OR 9 FOR FULLTEXT)

SWIFT rolls out security package

Anonymous

Banking World, v 12, n 3, p 31-33, Mar 1994 Document Type: Journal Article Language: English Record

Type: Abstract Fulltext Word Count: 00695

Abstract:

....of smart cards will guarantee the identity of the sender and remove the need for **secret information** to be sent through the mail.

Under the User Security Enhancemen program, some 16,000...

...of smart cards will guarantee the identity of the sender and remove the need for **secret information** to be sent through the post. The SWIFT secretariat will be able to transmit tables of **access codes** to member banks across the network. And member banks will use the network itself to exchange bilateral **authentication** keys.

Under the USE programme some 16,000 readers (a basic reader for access and...

...the tedious requirement for dealing with paper-based correspondence. And with the smart card reader, 'secret' data need never be displayed to human eyes. Bilateral keys will be digitally signed; this enables the receiver to authenticate the true identity of the sender."

The roll-out is proceeding on a phased basis...

...will also mean a drastic decrease in the workload involved in bilateral key exchanges. Supposedly **secret information** will no longer be visible to human eyes. But it will be expensive. In addition...

...computer interfaces with the network and there will be on-going costs for the bilateral **key** exchange system. Security has its price."

20/3,K/8 (Item 1 from file: 267) Links
Finance & Banking Newsletters
(c) 2007 Dialog. All rights reserved.
04543331
Web site success starts with security

Jane Paradiso

Employee Benefit News

December 1,1998 **Document Type:** NEWSLETTER **Publisher:** SECURITIES DATA PUBLISHING

Language: ENGLISH Word Count: 824 Record Type: FULLTEXT

(c) SECURITIES DATA PUBLISHING All Rts. Reserv.

Text:

...the secure socket layer protocol. SSL is an open, non-proprietary protocol that provides privacy, authentication and reliability but not always positive identification.

Transmissions between users over an SSL network are private because each user has a **secret key** that encrypts the **data**. The U.S. version uses a difficult-to-crack 128-bit algorithm for data encryption...

...does allow a much less robust 40-bit version to be exported.

SSL communications are authenticated because each party can verify
each other's identity using standard public key algorithms. This
does not, however, safeguard against individuals who have falsely gained
another identity. SSL...be attributed to an individual but also can be
stolen or discovered by hackers. A PIN is a "secret key"
known to both the user and the system to gain and validate access using one

...a complementary set of matched keys, private and public, to ensure positive identification. Your private **key** resides on your server and can be only accessed by you. Your public **key** is widely disseminated and can be used by others to encrypt information sent to you. You then decode the information using your private **key**.

In the reverse, information you create with the private **key** contains your digital signature, which can be decoded only with your public **key** to verify the digital signature. Your private **key** cannot be derived from the public **key**, so it's safe from theft by hackers.

Companies that provide this software refer to it as public **key** infrastructure or PKI. Two of the largest vendors are VeriSign (www.verisign.com) and Entrust...

20/3,K/9 (Item 2 from file: 267) <u>Links</u>

Finance & Banking Newsletters (c) 2007 Dialog. All rights reserved.

04540628

The Latest Link: Linked benefit products combine the advantages of life insurance and long-term care in one policy.

Thomas W. Fitch
Bank Investment Marketing

October 1,1998 Document Type: NEWSLETTER Publisher: SECURITIES DATA PUBLISHING

Language: ENGLISH Word Count: 1234 Record Type: FULLTEXT

(c) SECURITIES DATA PUBLISHING All Rts. Reserv.

...address one of their most significant concerns - the need for long-term care - in a **unique** way. It's no **secret** that the **number** of people over the age of 55 is growing in unprecedented ways, and the trend...

Text:

...address one of their most significant concerns - the need for long-term care - in a **unique** way. It's no **secret** that the **number** of people over the age of 55 is growing in unprecedented ways, and the trend...

...an uncertain future, living longer poses additional challenges - personal and financial - for older adults. A **key** question is how to manage financial resources to strike a balance between enjoying life and...

20/3,K/10 (Item 3 from file: 267) <u>Links</u> Finance & Banking Newsletters (c) 2007 Dialog. All rights reserved.

00037657

CONCERN AWAITS ATMs THAT USE BIOMETRICS Diebold Debuts Facial, Voice Scans At BAI Retail Delivery Conference '97

EFT REPORT

December 3, 1997 Vol: 20 Issue: 24 Document Type: NEWSLETTER

Publisher: PHILLIPS BUSINESS INFORMATION

Language: ENGLISH Word Count: 1062 Record Type: FULLTEXT

(c) PHILLIPS PUBLISHING INTERNATIONAL All Rts. Reserv.

Text:

...U.S. market.

The public's receptiveness to having body parts take the place of personal identification number-based cards at the ATM,

however, is an

unknown. Battle lines, nevertheless, are being drawn.

Vendors and biometric advocates sing the praises of a body part's ultimate authentication of a user, and the convenience of a passive, silent scan. Civil libertarians, however, raise...

...to secure their assets," Atick says. "They recognize they can lose their

card and their **PIN** is not safe. At the end of the day, you have to justify the use...in many cases we don't," he says. "One possible objection is when [the scanned **information**] is shared across databases

your anonymity will be intruded upon, where historically you were able

to be anonymous. In some future...

20/3,K/11 (Item 4 from file: 267) Links Finance & Banking Newsletters (c) 2007 Dialog. All rights reserved. 00009469 MC Securities, Rudloff's last crusade

Euromoney Magazine

July 1996 00, Page: 38, 041 Document Type: NEWSLETTER Publisher: EUROMONEY ELECTRONIC PUBLICATIONS

Language: ENGLISH Word Count: 3923 Record Type: FULLTEXT

(c) EUROMONEY ELECTRONIC PUBLICATIONS All Rts. Reserv.

Text:

...in Moscow and 55 in Prague.

But Rudloff readily admits to a flaw in one **key** area of his strategy. An ideas man - some of his best are apparently dreamed up...all, six partners have left. New ones joined, so there are now 11, including an **undisclosed number** of the eight founding partners. One of the early departures was Stuart Lucas, who for...deputy chairman of Swiss drugs company Novartis, formerly Sandoz and Ciba-Geigy.)

Impressive performance

A **key** part of equity capital markets is the sales force in Geneva, which should come as...business will be channelled via MC's London headquarters.

Equity stake

But the deal's **key** benefit for BBL is its majority control of a large eastern European operation. "Outside of...locals, has only eight expatriates. The heavy weighting in Russians is aptly reflected by a **sign on** the stairs saying "Cigarettes Only". Downstairs in a homely corporate kitchen the heavy smokers can...

20/3,K/12 (Item 1 from file: 608) Links

KR/T Bus.News.

(c)2007 Knight Ridder/Tribune Bus News. All rights reserved.

00300833 Story Number: 15404 (USE FORMAT 7 OR 9 FOR FULLTEXT)

THE MIAMI HERALD CYBERGUIDE COLUMN

Dan Keating The Miami Herald October 6, 1995 14:04 E.T.

Document Type: Newspaper Record Type: Fulltext Language: English

Word Count: 975

Text:

...of you who will dig in that way, here are the biggies.
For ftp, use "anonymous" as your login name when
signing on to the site
and use your e-mail address as the password. Then use "cd" to move forward to
a specified directory, such as "cd pub" to...